PÔLE D'EXCELLENCE CYBER

Guide

Nos étudiants ont du talent !

Pourquoi recruter un stagiaire ou un alternant en cyber ?

Septembre 2026

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS

Liberté
Égalité
Fraternité

SOMMAIRE

Préface 5

Introduction 6

Fiche 1 : Inventorier et mieux connaître son système d'information 8

Fiche 2 : Élaborer une politique de sécurité des systèmes d'informations (PSSI) 9

Fiche 3 : Gérer les fournisseurs et les prestataires 10

Fiche 4 : Gérer les accès et les profils utilisateurs 11

Fiche 5 : Maintenir en conditions opérationnelles 12

Fiche 6 : Contrôler les accès physiques et logiques 13

Fiche 7 : Concevoir et déployer une architecture sécurisée 14

Fiche 8 : Sécuriser les accès distants 15

Fiche 9 : Protéger les systèmes d'information contre les codes malveillants (Malware) 16

Fiche 10 : Gérer les identités et les accès 17

Fiche 11 : Sécuriser l'administration des systèmes d'information 18

Fiche 12 : Identifier et réagir aux incidents de sécurité 19

Fiche 13 : Garantir la continuité et la reprise d'activité 20

Fiche 14 : Piloter la réaction aux crises d'origine cyber 21

Fiche 15 : Organiser des exercices, tests et entraînements de cybersécurité 22

Fiche 16 : Piloter une approche par les risques 23

Fiche 17 : Auditer la sécurité des systèmes d'information 24

Fiche 18 : Sécuriser les configurations des systèmes d'information 25

Fiche 19 : Administrer les systèmes d'information depuis des ressources dédiées 26

Fiche 20 : Superviser la sécurité des systèmes d'information 27

Exemples de missions confiées à des stagiaires ou alternants 28

Points de repères sur le cadre réglementaire des stages et contrats d'alternance 30

Par où commencer pour trouver un stagiaire ou alternant en cybersécurité ? 32

Conclusion 34

Synthèse des fiches 36

PRÉFACE

Par David MENIER, Président de l'Université Bretagne Sud
VP Formation du Pôle d'excellence cyber (PEC)

En ce début d'année 2026, alors que les cybermenaces redessinent les contours de notre sécurité collective, une évidence s'impose : la cybersécurité n'est plus une option, mais une nécessité. Pour nos entreprises, nos collectivités, nos institutions, la question n'est plus si elles seront ciblées, mais quand. Face à ce constat, une autre question émerge, tout aussi cruciale : où trouver les talents capables de nous protéger ?

La réponse, le **Pôle d'Excellence Cyber** et ses partenaires vous la proposent aujourd'hui à travers ce guide : **nos étudiants ont du talent**. Encore faut-il leur en donner l'occasion.

Fruit d'une collaboration étroite entre acteurs académiques, entreprises et institutions, cet ouvrage est un pont entre l'urgence des besoins et l'énergie des compétences de demain. Avec ses 20 fiches missions, il offre aux organisations, qu'elles soient PME, collectivités ou grands groupes, des solutions concrètes pour intégrer des étudiants en cybersécurité, selon leur niveau de formation. Inventaire des systèmes d'information, élaboration de politiques de sécurité, gestion des incidents ou supervision des réseaux : autant de missions qui, bien encadrées, permettront aux entreprises de monter en maturité cyber, tout en offrant aux étudiants une expérience professionnelle formatrice.

La Bretagne, avec son écosystème dynamique et le Pôle d'excellence cyber avec son réseau de plus de 135 membres ont su fédérer les forces vives pour répondre à ce défi. Mais l'enjeu dépasse nos frontières régionales. Il concerne toute la France, et même au-delà. Car la cybersécurité est l'affaire de tous : entreprises, institutions, citoyens. Et c'est ensemble que nous bâtirons une souveraineté numérique résiliente.

Je suis convaincu que l'alliance entre formation, innovation et terrain est la clé pour relever ce défi. Les étudiants que nous formons aujourd'hui sont les gardiens du numérique de demain. Leur talent, leur créativité et leur engagement sont des atouts précieux pour nos organisations.

David Menier

Président de l'Université Bretagne Sud

Vice-Président Formation du Pôle d'excellence cyber

Professeur des Universités

INTRODUCTION

La cybersécurité est aujourd'hui devenue un enjeu majeur pour l'ensemble des organisations. Qu'il s'agisse de grandes entreprises, de collectivités, d'établissements publics, de PME ou de TPE, toutes sont confrontées à la nécessité de protéger leurs systèmes d'information, leurs données et leurs activités face à des menaces toujours plus nombreuses et sophistiquées. Dans le même temps, les besoins en compétences dans ce domaine ne cessent de croître, créant une demande forte de professionnels formés capables d'accompagner cette montée en maturité cyber.

Pourtant, alors même que les formations se développent et que de nombreux étudiants choisissent cette filière porteuse d'avenir, l'accès aux stages et à l'alternance demeure une difficulté importante. Cette situation s'explique en partie par un contexte économique et conjoncturel complexe : réduction de certaines aides à l'embauche des alternants, ralentissement économique dans plusieurs secteurs, incertitudes géopolitiques ou encore prudence accrue des entreprises dans leurs recrutements. Ces facteurs limitent mécaniquement le nombre de postes proposés aux étudiants.

La cybersécurité concerne toutes les entreprises.

Face à cette situation, un groupe de travail du Pôle d'Excellence Cyber a souhaité s'interroger sur les leviers d'actions disponibles. Une évidence s'est rapidement imposée : les entreprises spécialisées en cybersécurité connaissent déjà les formations existantes et recrutent régulièrement des stagiaires ou alternants. Cependant, elles ne pourront pas, à elles seules, accueillir l'ensemble des étudiants formés chaque année.

Dans le même temps, la cybersécurité n'est plus une préoccupation réservée aux spécialistes du secteur. Toutes les organisations, quels que soient leur taille ou leur domaine d'activité, doivent aujourd'hui renforcer leur sécurité numérique, améliorer leurs pratiques et répondre à des exigences réglementaires et opérationnelles de plus en plus fortes.

L'enjeu consiste donc à élargir le vivier des entreprises susceptibles d'accueillir des étudiants en cybersécurité et à faire connaître les bénéfices qu'elles peuvent retirer de cette collaboration avec des apprenants.

Les étudiants ont des compétences utiles et immédiatement mobilisables

Les étudiants en cybersécurité représentent un potentiel important pour les organisations. Au cours de leur formation, ils développent des compétences techniques, méthodologiques et organisationnelles qui peuvent contribuer concrètement à l'amélioration du niveau de sécurité d'une entreprise.

Selon leur niveau d'études, ils peuvent intervenir sur des missions variées. Ainsi, les étudiants préparant un diplôme de niveau Bac+2 ou Bac+3 pourront davantage intervenir sur des missions opérationnelles nécessitant des compétences techniques et une mise en œuvre concrète. Les étudiants de niveau Bac+5 seront, quant à eux, davantage en mesure de contribuer à des travaux de conception, de gouvernance, de stratégie, de gestion des risques ou d'élaboration de politiques de sécurité, tout en mobilisant leurs connaissances techniques.

Bien entendu, chaque étudiant possède son propre parcours et son propre niveau d'autonomie. Les indications présentées dans ce guide constituent des repères généraux et non des frontières strictes. Certains étudiants pourront démontrer des compétences avancées très tôt dans leur cursus, tandis que d'autres nécessiteront davantage d'accompagnement.

Dans tous les cas, ces étudiants ont besoin d'un tuteur de stage ou d'alternance qui est soit diplômé du même niveau que le diplôme préparé par l'apprenant, soit qui a au moins 2 ans d'expérience dans un poste similaire. Cet accompagnement par un professionnel au sein de l'entreprise est essentiel pour leur permettant d'apprendre, de monter en compétences tout en apportant une contribution réelle à l'organisation qui les accueille.

L'ambition de ce guide : rapprocher les besoins des entreprises et les talents des étudiants d'aujourd'hui qui seront les professionnels de demain.

Pour aider les entreprises à identifier les missions qu'elles peuvent confier à un étudiant, le groupe de travail s'est appuyé sur deux référentiels de l'ANSSI : les 42 mesures d'hygiène informatique et les recommandations associées à la directive NIS2. Le croisement de ces deux référentiels a permis d'identifier des actions concrètes pouvant être confiées à des étudiants selon leur niveau de formation.

Ce document a été conçu comme un outil pratique et accessible. Les employeurs peuvent y trouver des idées de missions adaptées à leurs besoins et à leur niveau de maturité cyber. Les étudiants peuvent, quant à eux, s'en servir pour mieux valoriser leurs compétences et illustrer ce qu'ils sont capables de réaliser en situation professionnelle.

Il ne s'agit pas d'un programme à appliquer dans son intégralité ni d'une liste exhaustive de tâches à confier à une seule personne. Ce guide se consulte librement : chacun peut y puiser une ou plusieurs idées pour construire un stage, une alternance ou un projet adapté à son contexte.

Parce que les entreprises ont besoin de renforcer leur cybersécurité et parce que les étudiants ont besoin d'opportunités pour développer leurs compétences, ce guide a pour vocation de faciliter cette rencontre. Car nos étudiants ont du talent ; encore faut-il leur donner l'occasion de le montrer.

Fiche mission n°1. Inventorier et mieux connaître son système d'information

Pourquoi cette mission est-elle importante ? Peut-on protéger ce que l'on ne connaît pas ? Dans de nombreuses organisations, il est difficile de répondre précisément à ses questions essentielles :

- Combien d'ordinateurs sont réellement utilisés ?
- Quels serveurs sont encore en production ?
- Quels logiciels sont installés ?
- Qui dispose de droits administrateur ?
- Les schémas réseau sont-ils à jour ?

Pourtant, disposer d'une vision claire de son système d'information constitue la première étape de toute démarche de cybersécurité. Sans inventaire fiable, il devient difficile d'appliquer les correctifs, de gérer les risques ou encore de répondre aux exigences réglementaires.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

Un étudiant peut notamment :

- Recenser les équipements informatiques (postes, serveurs, smartphones, imprimantes...)
- Identifier les utilisateurs et les principaux droits d'accès
- Vérifier et mettre à jour les schémas réseau existants
- Identifier les applications et logiciels utilisés
- Constituer ou mettre à jour une base d'inventaire des actifs
- Documenter l'architecture du système d'information

Niveau Bac+4 / Bac+5

Selon son niveau d'autonomie, un étudiant pourra également :

- Automatiser les inventaires (PowerShell, Python...)
- Concevoir une cartographie détaillée du système d'information
- Identifier les actifs critiques nécessitant une protection renforcée
- Réaliser un audit de cohérence entre l'inventaire et la réalité du terrain
- Formuler des recommandations pour améliorer la gouvernance du système d'information

Les bénéfices pour votre entreprise

À l'issue de cette mission, vous disposez notamment :

- d'un inventaire fiable de votre parc informatique ;
- d'une vision claire de vos actifs numériques ;
- d'une documentation technique mise à jour ;
- d'une meilleure maîtrise des comptes et des équipements sensibles ;
- d'une base de travail indispensable pour toutes vos futures démarches cyber (analyse de risques, PCA/PRA, conformité NIS2, audits...).

Cette mission contribue directement à...

Objectif RECYF / NIS2 : Objectif de sécurité 1.

Guide d'hygiène numérique de l'ANSSI : Règle n°4

Fiche 2. Élaborer une politique de sécurité des systèmes d'information (PSSI)

La Politique de Sécurité des Systèmes d'Information (PSSI) constitue le document de référence qui définit les règles, les responsabilités et les bonnes pratiques permettant de protéger les données, les infrastructures et les services numériques d'une organisation. Son élaboration s'inscrit dans un cadre de gouvernance de la sécurité numérique et répond aux exigences réglementaires ainsi qu'aux référentiels de bonnes pratiques, notamment la norme ISO 27001. Les étudiants peuvent contribuer à différents niveaux selon leur degré d'autonomie et d'expertise.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Participer à la rédaction de procédures de sécurité (gestion des mots de passe, sauvegardes, gestion des accès, bonnes pratiques).
- Contribuer à l'élaboration ou à la mise à jour de la PSSI à partir des besoins de l'organisation.
- Organiser ou animer des actions de sensibilisation des collaborateurs à la cybersécurité.
- Participer à l'identification des écarts de sécurité et à la rédaction de comptes rendus ou de rapports.
- Contribuer au suivi des actions correctives en lien avec les équipes techniques.

Niveau Bac+5

- Élaborer une PSSI cohérente avec la stratégie de l'entreprise et alignée sur les exigences de la norme ISO 27001.
- Définir le cadre de gouvernance de la cybersécurité : rôles, responsabilités, processus de décision et de contrôle.
- Piloter les plans d'actions visant à corriger les écarts de conformité et à améliorer le niveau de sécurité.
- Évaluer les risques liés à l'infogérance et proposer les mesures de maîtrise adaptées.
- Concevoir et piloter une stratégie de sensibilisation durable des utilisateurs et accompagner le changement.

Bénéfices pour l'entreprise

- Renforcement de la protection des systèmes d'information et des données.
- Réduction des risques de cyberattaques et d'erreurs humaines.
- Amélioration de la conformité réglementaire et de l'alignement avec les référentiels de sécurité.
- Clarification des responsabilités et des processus de gouvernance.
- Développement d'une culture de cybersécurité partagée par l'ensemble des collaborateurs.
- Amélioration continue de la maîtrise des risques, notamment dans le cadre de prestations d'infogérance.

Cette mission contribue à

Objectif RECYF / NIS2 : Objectif de sécurité 2.

Guide d'hygiène numérique de l'ANSSI : Règle 3, 33, 34,37, 39, 40, 42

Fiche 3. Gérer les fournisseurs et les prestataires

Les entreprises s'appuient de plus en plus sur des services externalisés (infogérance, cloud, maintenance, développement, hébergement), ce qui nécessite une maîtrise des risques associés. Une gestion rigoureuse des relations fournisseurs permet de garantir le respect des exigences de sécurité, de conformité et de continuité des activités tout au long du cycle de vie des prestations.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Maintenir à jour une liste exhaustive des fournisseurs et prestataires informatiques.
- Vérifier que les contrats de prestation intègrent les exigences de sécurité définies par l'entreprise.
- Participer au suivi des audits et à l'analyse des rapports simples concernant les services externalisés.
- Contribuer à la collecte des éléments de conformité demandés aux prestataires.
- Participer au suivi des actions correctives en lien avec les équipes internes et les fournisseurs.

Niveau Bac+5

- Élaborer des politiques de sécurité encadrant les relations avec les fournisseurs et les prestataires.
- Superviser les audits de conformité des prestataires et analyser les résultats.
- Évaluer les risques liés à l'infogérance et aux services externalisés.
- Définir des indicateurs de performance et de conformité (KPI) pour mesurer le respect des exigences contractuelles et de sécurité.
- Accompagner les directions métiers dans le pilotage des fournisseurs stratégiques et dans l'amélioration continue de leur niveau de sécurité.

Bénéfices pour l'entreprise

- Meilleure maîtrise des risques liés aux prestations externalisées.
- Renforcement de la conformité contractuelle et réglementaire.
- Amélioration du suivi des fournisseurs et de leur niveau de sécurité.
- Réduction des risques de compromission provenant de la chaîne de sous-traitance.
- Amélioration de la qualité des prestations grâce à un pilotage fondé sur des indicateurs.
- Renforcement de la confiance entre l'entreprise et ses partenaires.

Cette mission contribue à

RéCyF /NIS 2 : Objectif de sécurité 3.

ANSSI : Règle 3

Fiche 4. Gérer les accès et les profils utilisateurs

La gestion des accès et des profils utilisateurs garantit que chaque collaborateur dispose uniquement des droits nécessaires à ses missions, tout en assurant une gestion sécurisée des arrivées, des départs et des changements de fonction.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Créer, modifier et supprimer les comptes utilisateurs ainsi que les droits d'accès associés.
- Maintenir à jour la documentation des profils utilisateurs et des autorisations.
- Participer à la sensibilisation des nouveaux collaborateurs aux bonnes pratiques de cybersécurité.
- Contribuer à l'application des procédures d'arrivée, de mobilité interne et de départ des collaborateurs.
- Vérifier la cohérence des droits attribués en fonction des besoins métiers.

Niveau Bac+5

- Concevoir et déployer un système de gestion des identités et des accès (IAM).
- Réaliser des audits détaillés des comptes utilisateurs et des droits d'accès.
- Définir les règles de gestion des habilitations selon le principe du moindre privilège.
- Superviser et optimiser les processus d'intégration, de mobilité et de départ des collaborateurs en conformité avec les politiques de sécurité.
- Mettre en place des indicateurs de suivi et proposer des améliorations des processus de gestion des accès.

Bénéfices pour l'entreprise

- Réduction des risques liés aux accès non autorisés.
- Renforcement de la protection des données et des ressources informatiques.
- Amélioration de la conformité avec les exigences réglementaires et les politiques internes.
- Gestion plus efficace du cycle de vie des comptes utilisateurs.
- Diminution des risques d'erreurs ou d'usurpation d'identité.
- Renforcement de la sensibilisation des collaborateurs à la cybersécurité.

Cette mission contribue à

RéCyF : Objectif de sécurité 4. Sécurité et ressources humaines

ANSSI : Règle 2, 6.

Fiche 5. Maintenir en conditions opérationnelles

Le maintien en conditions opérationnelles (MCO) vise à garantir la disponibilité, la sécurité et la résilience des systèmes d'information. Il repose sur une surveillance continue des infrastructures, la gestion des correctifs de sécurité, le suivi des comptes à privilèges et la maîtrise des vulnérabilités afin de limiter les risques de compromission.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Identifier les comptes privilégiés (administrateurs, super-utilisateurs) et vérifier la cohérence de leurs droits d'accès.
- Appliquer les mises à jour et correctifs de sécurité sur les postes de travail et les serveurs.
- Réaliser des scans de vulnérabilités sur les systèmes critiques et analyser les premiers résultats.
- Tester les procédures de sauvegarde et de restauration des données.
- Documenter les opérations réalisées et assurer le suivi des actions de maintenance.

Niveau Bac+5

- Superviser la gestion des mises à jour des systèmes critiques et définir les priorités de déploiement.
- Automatiser le suivi des vulnérabilités, des correctifs et des niveaux de conformité à l'aide d'outils spécialisés.
- Piloter la gestion des comptes à privilèges conformément aux bonnes pratiques de sécurité.
- Analyser les résultats des audits techniques et proposer des plans d'amélioration.
- Définir des actions visant à renforcer la sécurité, la disponibilité et la résilience des systèmes critiques.

Bénéfices pour l'entreprise

- Renforcement de la disponibilité et de la fiabilité des systèmes d'information.
- Réduction des risques liés aux vulnérabilités et aux cyberattaques.
- Meilleure maîtrise des comptes à privilèges et des accès sensibles.
- Amélioration de la continuité d'activité grâce à des sauvegardes maîtrisées.
- Optimisation des opérations de maintenance et de gestion des correctifs.
- Renforcement de la résilience des infrastructures informatiques.

Cette mission contribue à

RéCyF : Objectif de sécurité 5.

ANSSI : Règle 5

Fiche 6. Contrôler les accès physiques et logiques

Le contrôle d'accès physique et logique permet de protéger les locaux, les équipements et les ressources numériques contre les accès non autorisés. Il combine des mesures organisationnelles, techniques et humaines afin de garantir que seules les personnes et les équipements autorisés puissent accéder aux infrastructures de l'entreprise.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Enregistrer et gérer les accès physiques à l'aide de badges, registres ou serrures électroniques.
- Contrôler les accès aux salles serveurs, locaux techniques et zones sensibles.
- Participer à l'installation et à la mise en service de dispositifs de vidéosurveillance ou d'alarmes sous la supervision d'un responsable.
- Vérifier que seuls les équipements autorisés sont connectés au réseau de l'entreprise.
- Assurer le suivi et la mise à jour de la documentation relative aux accès physiques et aux équipements autorisés.

Niveau Bac+5

- Concevoir et déployer des dispositifs avancés de contrôle d'accès et de surveillance des locaux critiques (vidéosurveillance intelligente, biométrie, contrôle d'accès centralisé).
- Superviser les audits de sécurité physique des sites sensibles.
- Définir les politiques de contrôle d'accès physique et logique en cohérence avec la stratégie de sécurité de l'entreprise.
- Évaluer les risques liés aux accès physiques et proposer des mesures d'amélioration.
- Piloter les projets d'évolution des dispositifs de sécurité des infrastructures critiques.

Bénéfices pour l'entreprise

- Protection renforcée des locaux, des infrastructures et des équipements sensibles.
- Réduction des risques d'intrusion, de vol ou de sabotage.
- Maîtrise des accès aux zones critiques et aux équipements stratégiques.
- Amélioration de la traçabilité des accès physiques et des équipements connectés.
- Renforcement de la conformité avec les politiques de sécurité et les exigences réglementaires.
- Meilleure protection du système d'information contre les menaces internes et externes.

Cette mission contribue à

RéCyF : Objectif de sécurité 6.

ANSSI : Règle 26

Fiche 7. Concevoir et déployer une architecture sécurisée

Une architecture sécurisée permet de protéger les systèmes d'information en limitant les risques de compromission dès leur conception. Elle repose sur des principes tels que la réduction de la surface d'attaque, le cloisonnement des réseaux et la sécurisation des flux afin de renforcer la résilience des infrastructures.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Installer et configurer des équipements de sécurité réseau (pare-feu, systèmes de détection d'intrusion – IDS).
- Segmenter les réseaux afin de limiter les accès non autorisés et réduire les risques de propagation d'une attaque.
- Participer à l'intégration de nouvelles solutions réseau en vérifiant le respect des exigences de sécurité.
- Réaliser des tests de fonctionnement et de sécurité sur les infrastructures réseau.
- Documenter les configurations, les règles de filtrage et les procédures de mise en œuvre.

Niveau Bac+5

- Concevoir des architectures réseau sécurisées intégrant des DMZ, des VLAN et des mécanismes de cloisonnement adaptés aux besoins de l'organisation.
- Déployer des solutions avancées de segmentation et de cloisonnement des systèmes d'information.
- Auditer les architectures existantes afin d'identifier les vulnérabilités et proposer des plans d'amélioration.
- Définir les règles d'architecture garantissant la réduction de la surface d'attaque et la sécurisation des flux réseau.
- Piloter des projets d'évolution des infrastructures en intégrant les exigences de cybersécurité dès la phase de conception.

Bénéfices pour l'entreprise

- Réduction de la surface d'attaque du système d'information.
- Limitation de la propagation des incidents grâce au cloisonnement des réseaux.
- Renforcement de la disponibilité et de la résilience des infrastructures.
- Meilleure protection des données et des services critiques.
- Amélioration de la conformité avec les bonnes pratiques de cybersécurité.
- Optimisation des performances et de la maîtrise des flux réseau.

Cette mission contribue à

RéCyF : Objectif de sécurité 7.

ANSSI : Règle 7, 19, 20, 21, 22, 23, 25

Fiche 8. Sécuriser les accès distants

La sécurisation des accès distants est indispensable pour permettre aux collaborateurs, partenaires et prestataires d'accéder aux ressources de l'entreprise en toute sécurité. Elle repose sur la mise en œuvre de solutions de connexion sécurisées, le contrôle des accès et la surveillance des activités afin de limiter les risques de compromission.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Configurer des VPN pour les utilisateurs distants.
- Appliquer les bonnes pratiques de sécurisation des connexions à distance (authentification, chiffrement, contrôle des accès).
- Configurer des restrictions d'accès pour les connexions externes selon les besoins de l'organisation.
- Vérifier le bon fonctionnement des accès distants et assister les utilisateurs.
- Documenter les procédures de configuration et de gestion des accès à distance.

Niveau Bac+5

- Déployer et administrer des solutions avancées d'accès distant, telles que le Zero Trust Network Access (ZTNA).
- Superviser les connexions distantes et mettre en œuvre des mécanismes de détection des comportements anormaux.
- Élaborer des politiques de gestion et de contrôle des accès distants à l'échelle de l'organisation.
- Définir les exigences de sécurité pour les accès nomades, le télétravail et les accès des prestataires.
- Piloter l'amélioration continue des solutions d'accès distant en fonction des risques et des évolutions technologiques.

Bénéfices pour l'entreprise

- Sécurisation des accès aux ressources de l'entreprise depuis l'extérieur.
- Réduction des risques de compromission des comptes et des systèmes.
- Protection des échanges de données grâce au chiffrement des communications.
- Renforcement du contrôle des accès des collaborateurs, partenaires et prestataires.
- Amélioration de la détection des usages anormaux ou malveillants.
- Accompagnement du télétravail et de la mobilité dans un cadre sécurisé.

Cette mission contribue à

RéCyF : Objectif de sécurité 8.

ANSSI : Règle 9, 18, 30, 31, 32

.

Fiche 9. Protéger les systèmes d'information contre les codes malveillants (Malware)

La protection contre les codes malveillants est un pilier essentiel de la cybersécurité. Elle vise à prévenir, détecter et traiter les menaces telles que les virus, ransomwares, chevaux de Troie ou logiciels espions grâce à des solutions de protection, de supervision et de réponse aux incidents.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Installer et configurer des solutions antivirus et EDR (Endpoint Detection & Response).
- Effectuer des scans réguliers afin de détecter les logiciels malveillants.
- Gérer les mises à jour des bases antivirales et vérifier le bon fonctionnement des outils de protection.
- Participer au traitement des alertes de sécurité de premier niveau.
- Documenter les incidents détectés et les actions correctives mises en œuvre.

Niveau Bac+5

- Concevoir et déployer des solutions avancées de détection et de réponse aux incidents (SIEM, EDR).
- Analyser les incidents liés aux logiciels malveillants afin d'identifier leur origine, leur impact et les mesures correctives à mettre en œuvre.
- Déployer des outils d'analyse comportementale permettant de détecter les menaces avancées.
- Définir les stratégies de protection des postes de travail et des serveurs contre les codes malveillants.
- Piloter l'amélioration continue des dispositifs de détection et de réponse aux incidents.

Bénéfices pour l'entreprise

- Réduction des risques d'infection par des logiciels malveillants.
- Détection plus rapide des menaces et limitation de leur propagation.
- Renforcement de la protection des postes de travail, serveurs et terminaux.
- Amélioration de la continuité des activités grâce à une réponse rapide aux incidents.
- Diminution des impacts financiers et opérationnels liés aux cyberattaques.
- Renforcement du niveau global de cybersécurité de l'organisation.

Cette mission contribue à

RéCyF : Objectif de sécurité 9.

ANSSI : Règle 7, 14, 15, 24.

Fiche 10. Gérer les identités et les accès

La gestion des identités et des accès (Identity and Access Management – IAM) garantit que chaque utilisateur accède uniquement aux ressources nécessaires à ses missions. Elle repose sur une administration rigoureuse des comptes, des droits et des mécanismes d'authentification afin de protéger les systèmes d'information contre les accès non autorisés.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Administrer les comptes utilisateurs, les groupes et les droits d'accès aux ressources.
- Configurer et surveiller les règles de gestion des mots de passe conformément aux politiques de sécurité.
- Modifier les éléments d'authentification par défaut des équipements et services lors de leur mise en service.
- Documenter les créations, modifications et suppressions des comptes et des habilitations.
- Vérifier la cohérence des droits attribués en fonction des rôles et des responsabilités des utilisateurs.

Niveau Bac+5

- Mettre en œuvre des politiques avancées d'authentification forte (MFA, biométrie, authenti-fication adaptative).
- Auditer et optimiser la gestion des identités, des habilitations et des droits d'accès à l'échelle de l'organisation.
- Superviser les comptes administrateurs, les accès à privilèges et les mécanismes de traçabilité des actions.
- Définir les politiques d'habilitation selon les principes du moindre privilège et de la séparation des rôles.
- Piloter l'évolution des solutions IAM afin de renforcer la sécurité et la conformité des accès.

Bénéfices pour l'entreprise

- Réduction des risques d'accès non autorisés aux ressources sensibles.
- Renforcement de la protection des données et des systèmes critiques.
- Amélioration de la traçabilité des actions des utilisateurs et des administrateurs.
- Renforcement de la conformité réglementaire et des politiques internes de sécurité.
- Réduction des risques liés aux mots de passe faibles ou aux comptes mal administrés.
- Simplification de l'administration des identités et des habilitations.

Cette mission contribue à

RéCyF : Objectif de sécurité 10.

ANSSI : Règle 8, 9, 10, 12, 13

Fiche 11. Sécuriser l'administration des systèmes d'information

L'administration sécurisée des systèmes d'information vise à protéger les accès techniques permettant de gérer les infrastructures critiques. Elle repose sur le cloisonnement des environnements d'administration, la maîtrise des comptes privilégiés et la traçabilité des actions afin de limiter les risques liés aux usages administratifs.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Configurer les postes d'administration en appliquant les bonnes pratiques de sécurité.
- Vérifier les accès des comptes administrateurs et contrôler la conformité des habilitations.
- Participer à la gestion des configurations des équipements et dispositifs de sécurité.
- Mettre en œuvre les règles de restriction des droits d'administration sur les postes de travail.
- Contrôler la présence et la qualité des mécanismes de journalisation des activités administratives.
- Documenter les procédures d'administration sécurisée et les configurations appliquées.

Niveau Bac+5

- Déployer des infrastructures dédiées et sécurisées pour l'administration des systèmes d'information.
- Concevoir et superviser des réseaux d'administration cloisonnés et protégés.
- Mettre en place des systèmes avancés de journalisation et de traçabilité des actions des administrateurs.
- Réaliser des audits réguliers des comptes administrateurs, des accès privilégiés et des systèmes critiques.
- Définir les politiques de sécurité liées à l'administration du SI (restriction des accès Internet, séparation des environnements, contrôle des privilèges).
- Piloter l'amélioration continue des dispositifs de sécurisation des accès administrateurs.

Bénéfices pour l'entreprise

- Réduction des risques liés aux compromissions de comptes administrateurs.
- Protection renforcée des systèmes critiques et des infrastructures sensibles.
- Amélioration de la traçabilité des actions réalisées sur le système d'information.
- Limitation des erreurs humaines lors des opérations d'administration.
- Renforcement de la conformité avec les bonnes pratiques de cybersécurité.
- Meilleure maîtrise des accès privilégiés et des environnements sensibles.

Cette mission contribue à

RéCyF : Objectif de sécurité 11.

ANSSI : Règle 11, 27, 28, 29

Fiche 12. Identifier et réagir aux incidents de sécurité

La gestion des incidents de sécurité permet à une organisation de détecter rapidement les événements suspects, de limiter leurs impacts et de rétablir les services affectés. Elle repose sur la collecte des journaux, l'analyse des alertes, l'application de procédures de réponse et l'amélioration continue des dispositifs de sécurité.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Collecter et analyser les journaux (logs) des composants critiques du système d'information.
- Participer à la détection des anomalies à l'aide d'outils de supervision et de solutions SIEM.
- Appliquer les procédures de réponse aux incidents (isolement d'une machine infectée, remontée d'alertes, premières actions correctives).
- Maintenir la documentation des incidents de sécurité rencontrés.
- Participer au suivi des actions réalisées après un incident.
- Contribuer à la mise à jour des procédures et des bases de connaissances sécurité.

Niveau Bac+5

- Coordonner une cellule de crise lors d'incidents de sécurité majeurs.
- Élaborer des rapports d'incidents détaillés incluant l'analyse des causes, les impacts et les mesures correctives.
- Superviser les dispositifs de détection et d'analyse des événements de sécurité.
- Définir et améliorer les procédures de gestion des incidents conformément aux besoins de l'organisation.
- Mettre en place une démarche d'amélioration continue basée sur l'analyse des incidents récurrents.
- Piloter les retours d'expérience (REX) afin de renforcer les dispositifs de prévention et de réaction.

Bénéfices pour l'entreprise

- Réduction du temps de détection et de réaction face aux incidents.
- Limitation de l'impact des cyberattaques sur les activités de l'entreprise.
- Amélioration de la visibilité sur les événements de sécurité.
- Renforcement de la capacité de réponse aux crises cyber.
- Capitalisation des retours d'expérience pour éviter la répétition des incidents.
- Amélioration continue du niveau de sécurité du système d'information.

Cette mission contribue à

RéCyF : Objectif de sécurité 12.

ANSSI : Règle 36, 40.

Fiche 13. Garantir la continuité et la reprise d'activité

La continuité et la reprise d'activité permettent à une organisation de maintenir ou de restaurer ses services essentiels après un incident majeur. Elles reposent sur l'identification des systèmes critiques, la mise en place de sauvegardes fiables et la préparation de plans de continuité et de reprise adaptés.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Tester les procédures de sauvegarde et de restauration des données.
- Participer à la mise à jour des logiciels et des systèmes afin de maintenir leur niveau de sécurité et de disponibilité.
- Documenter les procédures de reprise après sinistre.
- Participer à l'élaboration et à la mise à jour des plans de continuité et de reprise d'activité (PCA/PRA).
- Vérifier la conformité des sauvegardes avec les exigences de disponibilité de l'organisation.
- Contribuer à la réalisation de tests de restauration et à la formalisation des résultats.

Niveau Bac+5

- Élaborer, maintenir et tester des plans de continuité et de reprise d'activité (PCA/PRA).
- Identifier les systèmes, applications et données critiques nécessitant une reprise prioritaire.
- Définir les stratégies de reprise adaptées aux besoins métiers et aux exigences de sécurité.
- Superviser des exercices de reprise d'activité basés sur des scénarios réalistes.
- Analyser les résultats des tests PCA/PRA et proposer des axes d'amélioration.
- Piloter l'amélioration continue des dispositifs de résilience de l'organisation.

Bénéfices pour l'entreprise

- Réduction des impacts liés aux incidents majeurs et aux interruptions de service.
- Amélioration de la capacité de l'entreprise à restaurer rapidement ses activités.
- Protection renforcée des données critiques grâce à une politique de sauvegarde maîtrisée.
- Meilleure préparation face aux sinistres informatiques et cyberattaques.
- Renforcement de la résilience du système d'information.
- Garantie d'une meilleure continuité des activités métiers essentielles.

Cette mission contribue à

RéCyF : Objectif de sécurité 13.

ANSSI : Règle 37.

Fiche 14. Piloter la réaction aux crises d'origine cyber

La gestion de crise cyber permet à une organisation de réagir efficacement face à un incident majeur affectant ses activités, ses données ou ses infrastructures numériques. Elle repose sur une organisation structurée, des plans d'urgence adaptés et une coordination efficace des acteurs techniques, métiers et décisionnels.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Participer à la mise en œuvre des plans d'urgence en cas d'incident cyber.
- Contribuer au suivi des actions engagées pendant et après une crise.
- Participer à la collecte des informations nécessaires au suivi de l'incident.
- Documenter les événements, les décisions prises et les actions réalisées.
- Suivre l'application des mesures correctives et post-crise.
- Participer aux exercices de simulation de crise afin de tester les procédures existantes.

Niveau Bac+5

- Coordonner la réponse aux crises cyber en mobilisant les équipes techniques, métiers et dé-cisionnelles.
- Superviser l'organisation et le déroulement des exercices de simulation de crise.
- Élaborer des rapports stratégiques destinés aux directions présentant l'impact, les actions menées et les recommandations.
- Définir et améliorer les processus de gestion de crise cyber.
- Piloter les retours d'expérience (REX) afin d'améliorer la préparation et la résilience de l'organisation.
- Accompagner la prise de décision en situation de crise grâce à une analyse structurée des risques et impacts.

Bénéfices pour l'entreprise

- Amélioration de la capacité de réaction face aux cyberattaques majeures.
- Réduction des impacts opérationnels, financiers et organisationnels liés aux crises.
- Meilleure coordination entre les différents acteurs impliqués.
- Renforcement de la préparation grâce aux exercices et simulations régulières.
- Amélioration continue des processus de gestion de crise.
- Protection renforcée de la réputation et de la confiance des parties prenantes.

Cette mission contribue à

RéCyF : Objectif de sécurité 14.

ANSSI :

Fiche 15. Organiser des exercices, tests et entraînements de cybersécurité

Les exercices et entraînements de cybersécurité permettent de préparer les équipes à réagir efficacement face aux incidents et aux crises. Ils contribuent à tester les procédures existantes, identifier les points d'amélioration et renforcer la capacité de l'organisation à faire face aux menaces numériques.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Participer à des exercices de simulation d'incidents de sécurité.
- Appliquer les protocoles de tests définis sous la supervision des responsables sécurité.
- Documenter les résultats des exercices et les actions réalisées.
- Participer à l'analyse des écarts identifiés lors des simulations.
- Contribuer à la mise à jour des procédures à partir des retours d'expérience.
- Suivre la réalisation des tests liés aux dispositifs de sauvegarde et de reprise lorsque cela est nécessaire.

Niveau Bac+5

- Concevoir et piloter des scénarios d'exercices de simulation cyber adaptés aux risques de l'organisation.
- Évaluer la performance des équipes de réponse lors des exercices et analyser leur capacité de réaction.
- Superviser l'organisation d'entraînements impliquant les équipes techniques, métiers et déci-sionnelles.
- Identifier les axes d'amélioration et intégrer les actions correctives dans les processus de sécurité.
- Élaborer des rapports d'analyse présentant les résultats des exercices et les recommandations associées.
- Définir une démarche d'amélioration continue basée sur les retours d'expérience.

Bénéfices pour l'entreprise

- Amélioration de la préparation des équipes face aux incidents cyber.
- Validation de l'efficacité des procédures de sécurité et de gestion de crise.
- Identification des faiblesses organisationnelles et techniques avant un incident réel.
- Renforcement de la coordination entre les différents acteurs.
- Développement d'une culture de cybersécurité au sein de l'organisation.
- Amélioration continue de la résilience du système d'information.

Cette mission contribue à

RéCyF : Objectif de sécurité 15.

ANSSI : Règle 37.

Fiche 16. Piloter une approche par les risques

L'approche par les risques permet à une organisation d'identifier, d'évaluer et de traiter les menaces susceptibles d'affecter son système d'information. Elle contribue à prioriser les actions de sécurité en fonction des enjeux métiers, réglementaires et techniques.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Participer à des analyses de risques simples sous la supervision d'un responsable sécurité.
- Contribuer à l'évaluation des risques liés à la conformité réglementaire (NIS, RGPD, DO-RA).
- Identifier les vulnérabilités, menaces et impacts associés aux actifs du système d'information.
- Maintenir à jour la documentation des risques identifiés.
- Participer à la collecte des informations nécessaires aux analyses de risques.
- Contribuer au suivi des actions de réduction des risques.

Niveau Bac+5

- Réaliser des analyses de risques avancées selon des méthodes reconnues telles que EBIOS Risk Manager ou ISO 27005.
- Élaborer des matrices de risques permettant de prioriser les actions de traitement.
- Définir et piloter des plans d'atténuation des risques.
- Concevoir des tableaux de bord de suivi des risques à destination des directions.
- Accompagner les métiers dans l'identification des enjeux et impacts liés aux risques numériques.
- Mettre en place une démarche d'amélioration continue de la gestion des risques cybersécurité.

Bénéfices pour l'entreprise

- Meilleure visibilité sur les risques pesant sur le système d'information.
- Priorisation des investissements et actions de sécurité selon les enjeux réels.
- Amélioration de la conformité aux exigences réglementaires.
- Réduction de l'exposition aux menaces cyber.
- Aide à la prise de décision grâce à des indicateurs de pilotage adaptés.
- Renforcement de la gouvernance et de la maîtrise des risques numériques.

Cette mission contribue à

RéCyF : Objectif de sécurité 16.

ANSSI : Règle 41.

Fiche 17. Auditer la sécurité des systèmes d'information

L'audit de sécurité permet d'évaluer le niveau de protection d'un système d'information, d'identifier les vulnérabilités et de vérifier la conformité avec les exigences de sécurité et réglementaires. Il contribue à définir des actions correctives afin d'améliorer continuellement la posture de cybersécurité de l'organisation.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Effectuer des scans de vulnérabilités sur les réseaux, postes et systèmes.
- Participer à l'analyse des failles de sécurité identifiées.
- Compiler et documenter les résultats des audits sous la supervision d'un responsable sécurité.
- Identifier les écarts par rapport aux bonnes pratiques de cybersécurité.
- Contribuer au suivi des actions correctives issues des audits.
- Participer à l'évaluation des niveaux de conformité réglementaire et organisationnelle.

Niveau Bac+5

- Réaliser des audits avancés de sécurité, notamment des évaluations de conformité selon des référentiels tels que ISO 27001.
- Superviser des campagnes de tests d'intrusion (pentests) et analyser les résultats obtenus.
- Identifier et évaluer les non-conformités réglementaires et proposer des plans de remédiation.
- Élaborer des recommandations stratégiques à partir des constats d'audit.
- Piloter le suivi des actions correctives et mesurer leur efficacité.
- Accompagner l'organisation dans l'amélioration continue de son niveau de sécurité.

Bénéfices pour l'entreprise

- Identification proactive des vulnérabilités et des faiblesses de sécurité.
- Réduction des risques de compromission du système d'information.
- Amélioration de la conformité aux référentiels et réglementations applicables.
- Priorisation des actions correctives selon leur niveau de criticité.
- Renforcement de la confiance des clients, partenaires et parties prenantes.
- Amélioration continue de la maturité cybersécurité de l'organisation.

Cette mission contribue à

RéCyF : Objectif de sécurité 17.

ANSSI : Règle 17, 38

Fiche 18. Sécuriser les configurations des systèmes d'information

La sécurisation des configurations consiste à appliquer des règles de durcissement et des standards de sécurité afin de réduire les vulnérabilités liées aux systèmes, applications et équipements informatiques. Elle garantit un niveau de protection homogène sur l'ensemble du parc grâce à des configurations maîtrisées et contrôlées.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Configurer les postes de travail et équipements informatiques selon les bonnes pratiques de sécurité.
- Désactiver les configurations par défaut présentant des risques (comptes, services ou paramètres inutilisés).
- Participer à l'application des politiques de sécurité via des outils de gestion centralisée.
- Tester les configurations des systèmes avant leur mise en production.
- Vérifier la conformité des configurations appliquées avec les standards internes.
- Participer à la surveillance de l'intégrité des fichiers et paramètres de configuration de sécurité.

Niveau Bac+5

- Élaborer des guides de configuration sécurisée pour les systèmes, applications et équipe-ments.
- Superviser le déploiement de configurations avancées de sécurité sur les environnements in-formatiques.
- Auditer les configurations existantes afin d'identifier les écarts et les vulnérabilités.
- Définir des standards de durcissement adaptés aux différents environnements techniques.
- Mettre en place des mécanismes de contrôle et de suivi des configurations de sécurité.
- Proposer des plans de correction et d'amélioration continue des configurations.

Bénéfices pour l'entreprise

- Réduction des vulnérabilités liées aux mauvaises configurations.
- Harmonisation du niveau de sécurité sur l'ensemble du parc informatique.
- Meilleure maîtrise des changements techniques et des évolutions du système d'information.
- Diminution des risques liés aux services, logiciels ou paramètres inutilisés.
- Amélioration de la conformité avec les politiques de sécurité internes.
- Renforcement de la fiabilité et de la résilience des infrastructures.

Cette mission contribue à

RéCyF : Objectif de sécurité 18.

ANSSI : Règle 14, 16.

Fiche 19. Administrer les systèmes d'information depuis des ressources dédiées

L'administration des systèmes d'information depuis des ressources dédiées permet de protéger les opérations sensibles de gestion des infrastructures. Elle repose sur des environnements isolés, des accès nominatifs et des réseaux d'administration sécurisés afin de limiter les risques liés aux comptes privilégiés et aux actions d'administration.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Configurer les postes utilisés pour l'administration des systèmes d'information.
- Suivre et contrôler les accès aux environnements d'administration.
- Appliquer les bonnes pratiques de sécurisation des réseaux d'administration.
- Vérifier l'utilisation de comptes nominatifs et la séparation des rôles utilisateurs et administrateurs.
- Participer à la mise en œuvre des restrictions d'accès Internet sur les postes d'administration.
- Documenter les configurations et procédures liées aux ressources d'administration.

Niveau Bac+5

- Déployer des infrastructures dédiées à l'administration sécurisée des systèmes d'information.
- Concevoir et maintenir des réseaux d'administration cloisonnés et protégés.
- Mettre en œuvre des protocoles sécurisés pour l'administration locale et distante.
- Superviser les audits des activités d'administration et analyser les traces associées.
- Définir les politiques d'accès aux environnements d'administration en appliquant le principe du moindre privilège.
- Piloter l'amélioration continue des dispositifs de sécurisation des opérations d'administration.

Bénéfices pour l'entreprise

- Réduction des risques liés à la compromission des comptes administrateurs.
- Protection renforcée des infrastructures critiques.
- Meilleure traçabilité des opérations sensibles réalisées sur le système d'information.
- Limitation des erreurs et des usages non conformes lors des opérations d'administration.
- Renforcement du cloisonnement entre les environnements utilisateurs et administrateurs.
- Amélioration de la conformité avec les bonnes pratiques de cybersécurité.

Cette mission contribue à

RéCyF : Objectif de sécurité 19.

ANSSI : Règle 8, 27, 28.

Fiche 20. Superviser la sécurité des systèmes d'information

La supervision de la sécurité des systèmes d'information permet de détecter rapidement les événements suspects, d'analyser les comportements anormaux et de réagir face aux menaces. Elle repose sur la collecte des journaux, l'utilisation d'outils de surveillance et la mise en place de mécanismes de détection adaptés.

Ce qu'un étudiant peut réaliser

Niveau Bac+2 / Bac+3

- Utiliser les outils de supervision afin de surveiller les événements de sécurité.
- Collecter et analyser les journaux (logs) issus des principaux composants du système d'information.
- Gérer les alertes de sécurité et traiter les incidents de premier niveau.
- Documenter les activités de supervision et rédiger des rapports d'anomalies.
- Participer à la connexion des sources de logs vers une solution SIEM.
- Contribuer au filtrage et à la normalisation des données collectées pour faciliter leur analyse.

Niveau Bac+5

- Mettre en place et administrer des solutions avancées de supervision de sécurité (SIEM).
- Créer des règles de détection basées sur des seuils, des corrélations d'événements et des scénarios de menace.
- Automatiser l'analyse des logs et la corrélation des événements de sécurité.
- Optimiser les capacités de détection afin de réduire les faux positifs et améliorer la réactivité.
- Former et coordonner les équipes en charge de la supervision sécurité.
- Définir des indicateurs de suivi permettant d'améliorer la performance du dispositif de surveillance.

Bénéfices pour l'entreprise

- Détection plus rapide des menaces et des comportements suspects.
- Amélioration de la visibilité sur l'activité du système d'information.
- Réduction du temps de réaction face aux incidents de sécurité.
- Renforcement de la capacité d'analyse et d'investigation.
- Meilleure traçabilité des événements techniques et de sécurité.
- Amélioration continue du niveau de protection grâce à une supervision adaptée.

Cette mission contribue à

RéCyF : Objectif de sécurité 20.

ANSSI : Règle 36.

Exemples de missions confiées à des stagiaires ou alternants

Les différentes missions présentées dans les fiches descriptives se veulent combinatoires pour, en fonction des durées et des modalités, proposer des objectifs de stage/alternance répondant aux besoins de l'entreprise et aux attendus des référentiels de formation.

A titre d'illustration :

Contexte entreprise : PME de 25 salariés (1 référent informatique, service externalisé)

Type de contrat : Stage court de 2 mois / Formation niveau Bac +2

Missions confiées :

- Mission 1 : Inventorier, cartographier et documenter le système d'information (postes, serveurs, droits d'accès).
- Mission 4 : Gérer les accès utilisateurs (créer/supprimer des comptes, vérifier les droits).
- Mission 6 : Contrôler les accès physiques (badges, salles serveurs).

Bénéfices pour l'entreprise :

- Visibilité sur le parc informatique.
- Base solide pour des actions futures de sécurisation.
- Documentation mise à jour pour la conformité (NIS2, RGPD).

Exemple de livrable :

- Inventaire complet des actifs numériques.
- Liste des droits d'accès par utilisateur.
- Procédure de gestion des badges.

Contexte entreprise : Collectivité territoriale (150 collaborateurs, service informatique internalisé)

Type de contrat : Alternance sur 1 an / Formation niveau Bac+3

Missions confiées :

- Mission 2 : Élaborer une ébauche de Politique de Sécurité des Systèmes d'Information (PSSI).
- Mission 16 : Participer à une analyse de risques simple (matrice des risques).
- Mission 18 : Appliquer des configurations sécurisées sur les postes de travail (durcissement).

Bénéfices pour l'entreprise :

- Sensibilisation des équipes à la cybersécurité.
- Réduction des risques liés aux mauvaises configurations.
- Conformité avec les exigences réglementaires (NIS2 pour les collectivités).

Exemple de livrable :

- Ébauche de PSSI formalisée.
- Matrice des risques simplifiée.
- Guide de configuration sécurisée pour les postes.

Contexte entreprise : Grand compte industriel (500 salariés, service informatique structuré)

Type de contrat : Alternance sur 2 ans / formation de niveau Bac+5

Missions confiées :

- Mission 7 : Concevoir une architecture réseau sécurisée (segmentation, DMZ, cloisonnement).
- Mission 12 : Participer à la détection et réponse aux incidents (analyse des logs, qualification des alertes).
- Mission 17 : Réaliser un audit complet de sécurité (ISO 27001, tests d'intrusion).
- Mission 20 : Mise en place d'un outil de supervision et création de tableaux de bord.

Bénéfices pour l'entreprise :

- Réduction de la surface d'attaque grâce à une architecture sécurisée.
- Amélioration de la réactivité face aux incidents.
- Identification proactive des vulnérabilités avant les attaques.

Exemple de livrable :

- Schéma d'architecture réseau sécurisée (DMZ, VLAN).
- Rapport d'analyse des incidents (qualification des alertes).
- Audit de sécurité complet (ISO 27001, recommandations).

Points de repères sur le cadre réglementaire des stages et contrats d'alternance.

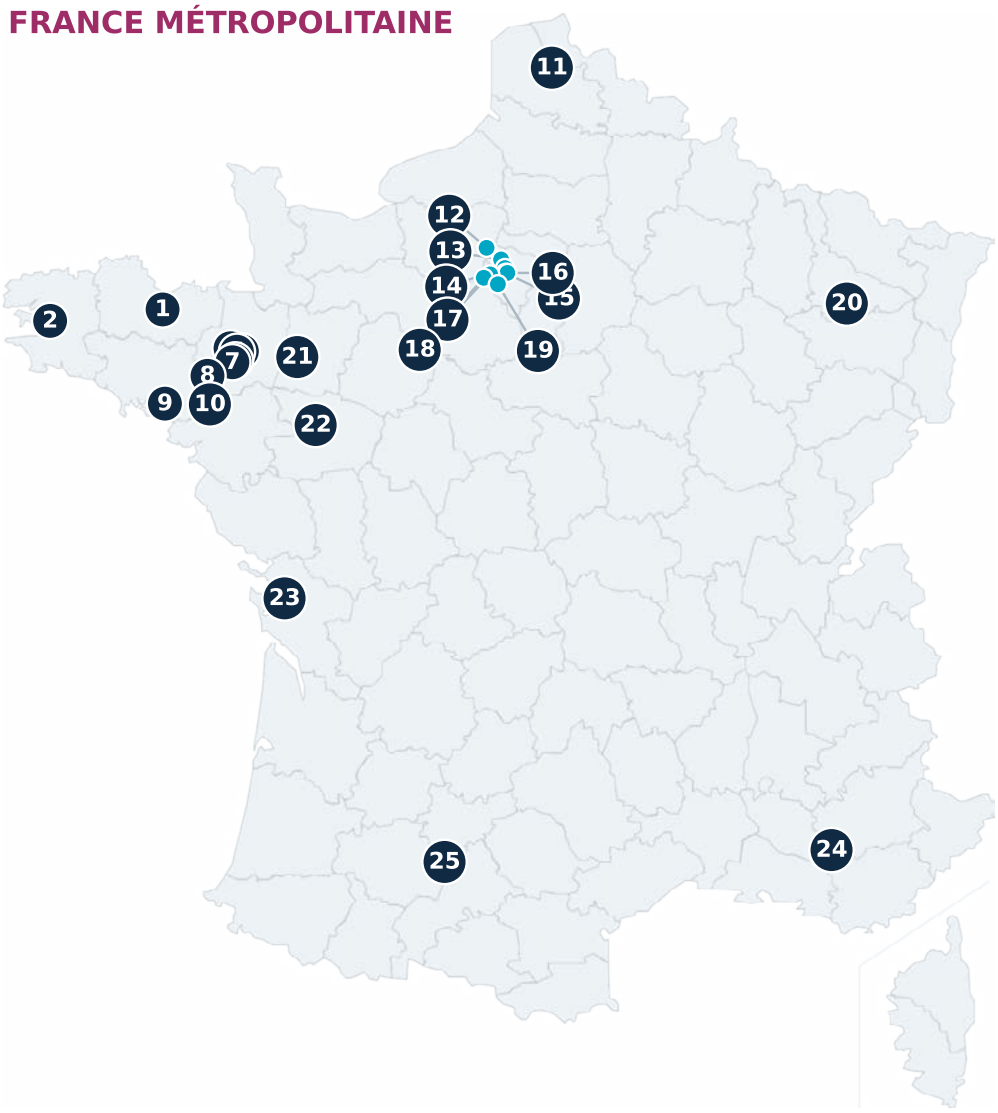
Le tableau ci-dessous vise à vous donner quelques éléments de repères différenciant entre stages et alternances. Bien évidemment ces éléments sont des ordres d'idées, chaque entreprise a souvent sa politique interne en la matière. De manière identique, chaque école a sa politique tarifaire. Néanmoins, ces éléments permettront de donner une évaluation globale des coûts à prendre en compte.

Type de contrat	Durée typique	Réglementation applicable	Coût pour l'entreprise	Exemple de formations.
Stage court	Moins de 2 mois consécutifs	- Pas de gratification obligatoire - Convention de stage obligatoire. - Pas de charges sociales patronales si respect des conditions.	Pas de coût minimum, gratification selon convention de l'entreprise	Parcours Qualif Emploi, Programme / Conseil Régional (publics en reconversion) / Jeunes en lycées, stages de découverte en licence 1 ou 2, ou BTS.
Stage court	De 2 mois consécutifs à 4 mois	- Gratification minimale (selon durée et année d'étude) : 15% du plafond horaire de la Sécurité Sociale (soit 5,60€/ heure en 2024). - Convention de stage obligatoire. - Pas de charges sociales patronales si respect des conditions.	Coût total : 1 000 à 2 000€ (selon durée et gratification).	BTS, BUT, Bachelors

Stage long	4 à 6 mois	- Gratification minimale : 15% du plafond horaire de la Sécurité Sociale (soit 5,60€/heure). - Convention de stage obligatoire. - Exonération de charges sociales patronales si gratification ≤ 15% du plafond horaire. - Si gratification > 15%, cotisations sociales réduites.	Coût total : 5 000 à 8 000€ (selon durée, gratification et exonérations).	Master ou école d'ingénieur en dernière année.
Alternance Bac+2	1 à 2 ans	- Rémunération selon l'âge et l'année d'études (entre 55% et 70% du SMIC). - Contrat d'apprentissage ou de professionnalisation. - Exonérations de charges sociales (selon type de contrat et taille de l'entreprise). - Aide financière possible (ex. : aide unique à l'apprentissage).	Coût total : 10 000 à 15 000€/an (selon formation, âge, rémunération et exonérations).	
Alternance Bac+5	1 à 2 ans	- Rémunération selon l'âge et l'année d'études (entre 65% et 80% du SMIC). - Contrat d'apprentissage ou de professionnalisation. - Exonérations de charges sociales (selon type de contrat et taille de l'entreprise). - Aides financières possibles (ex. : aide unique à l'apprentissage).	Coût total : 12 000 à 18 000€/an (selon formations, âge de l'alternant, rémunération et exonérations).	

Par où commencer pour trouver un stagiaire ou un alternant en cybersécurité ?

Les établissements et organismes de formation membres du Pôle d'excellence cyber forment, partout en France, des étudiants capables de contribuer concrètement à la sécurisation de votre organisation. Cette carte vous permet d'identifier les acteurs de notre réseau et de vous rapprocher d'eux pour trouver un profil adapté à vos besoins.



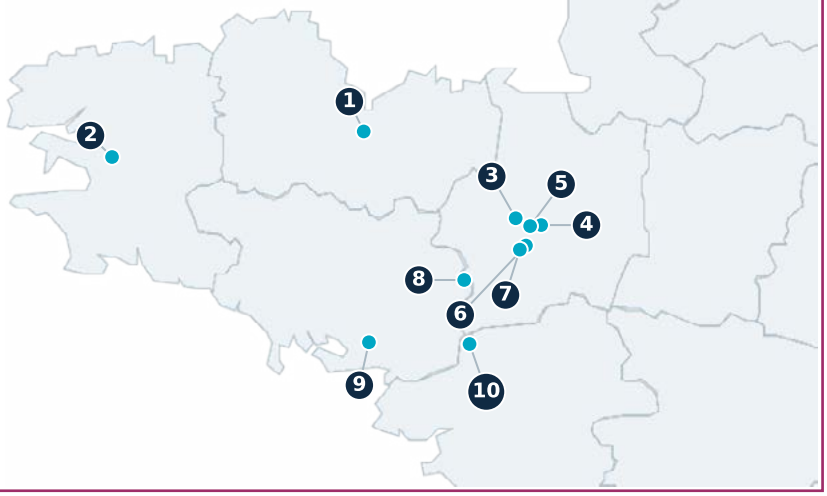
Cette cartographie présente les membres « Formation » du Pôle d'excellence cyber et ne constitue pas un recensement exhaustif des formations proposées en France.

LÉGENDE

Un numéro correspond à une implantation.

1. **Ploufragan**
   CNAM
2. **Brest**
   Université de Bretagne Ouest
   YNCREA ISEN Brest
   IMT Atlantique
   Ecole Navale
3. **Pacé**
   Ascent formation
4. **Cesson-Sévigné**
   ETNC – École des transmissions
   Centrale Sup Elec
5. **Rennes**
   Université de Rennes
   Sciences Po
   Rennes School of Business
   INSA Rennes
   Groupe Saint Jean
   ENS Rennes
   EPITA Rennes
6. **Chartres-de-Bretagne**
   ENI Ecole informatique
7. **Bruz**
   UIMM
   ENSAI
8. **Guer**
   ESCC
9. **Vannes**
   Université Bretagne Sud
   ENSIBS
10. **Redon**
    GIP CEI
11. **Lille**
    YNCREA ISEN
12. **Cergy**
    ESPTA
13. **Gennevilliers**
    Oteria Cyber School
14. **Paris**
    ECE
    ESTIAM
    ESGI
15. **Le Kremlin-Bicêtre**
    EPITA
16. **Ivry-sur-Seine**
    Ynov
    IPSA
17. **Versailles**
    École Hexagone
    EECS
18. **Montigny-le-Bretonneux**
    Ecole 2600
19. **Palaiseau**
    Polytechnique
    ENSTA I Institut polytechnique de Paris
20. **Molsheim**
    Ecole 18.06
21. **Laval**
    ESIEA
22. **Saint-Barthélemy-d'Anjou**
    ESAIP
23. **Rochefort-sur-Mer**
    EFSOAA
24. **Nice**
    Deep law for tech
25. **Toulouse**
    EPITA Toulouse

FOCUS BRETAGNE



Conclusion

Ce travail collectif est né de constats partagés dans différents groupes de travail du Pôle d'Excellence Cyber. Certains de ces groupes de travail sont mutualisés avec Bretagne Cyber Alliance, le campus cyber régional, et d'autres ont fait l'objet de nombreux échanges et réflexions au sein du projet Cyberskills4all (AMI CMA Breton). Les apprenants peinent de plus en plus à trouver des lieux d'accueil que ce soit pour des stages ou des alternances. La conjoncture économique, la baisse des aides de l'état sur l'alternance contribuent à cette difficulté, mais il faut sans doute aussi regarder l'état de maturité de la cybersécurité aujourd'hui pour mieux en comprendre les causes. L'âge d'or de la cybersécurité où les entreprises recrutaient massivement des profils correspondant partiellement à leurs besoins et qu'ils reformaient ensuite en interne est révolue. Les entreprises sont plus sélectives dans leurs choix car il y a plus de jeunes en recherche : ils peuvent se permettre d'être plus exigeants !

Les apprenants doivent donc changer leur stratégie de recherche de lieux de stages et d'alternance pour ne plus se tourner uniquement vers les entreprises spécialisées en cyber, mais en portant le regard vers toutes les entreprises qui ont besoin de se sécuriser. De leur côté, les entreprises doivent progresser dans leur démarche de cybersécurité, et des apprenants peuvent les aider à accélérer dans cette démarche. Si ces entreprises sont également accompagnées dans la priorisation des actions à mettre en place via tous les dispositifs existants (voir la page références), cette démarche peut être très efficace.

L'objectif de ce document est ainsi bien de répondre à ces défis :

- Mieux faire connaître les missions réalisables par des apprenants, selon le niveau de formation (Bac+2/3 vs Bac+4/5).
- Aider les entreprises non spécialisées à monter en maturité cyber en faisant appel à des étudiants qui, bien encadrés, pourront accélérer cette sécurisation.
- Mettre en relation entre les entreprises et les stagiaires/alternants.
- Comprendre et intégrer petit à petit les exigences réglementaires (comme la NIS2 ou les 42 recommandations d'hygiène numérique de l'ANSSI).

Vous l'avez compris, ce document se veut une source d'inspiration, de vulgarisation et de rapprochement entre les étudiants et les entreprises à sécuriser. Il n'est bien sûr pas exhaustif : de nombreuses autres missions peuvent être confiées à des apprenants, avec un encadrement de stage ou d'alternance solide.

Rédacteurs membres du groupe de travail opérationnel sur le sujet.

Michael ALLAIN
GRETA

Ana GUIMARD
Région Bretagne

Solène CHEVREAU
PEC

Jean LABOURDETTE
ENSIBS

Régine DIVÉRRÈS
We Ker

Paul André PINCEMIN
Rennes Métropole

Claire ETIENNE
GIP-FAR / Réseau des GRETA-CFA de bretagne

David VANKERSSCHAEVER
ESIEA

Nous souhaitons également remercier les participants qui nous ont rejoint ponctuellement sur une partie de ce travail :

- Julien BREYAULT, ENSIBS
- Olivier BUARD, ECE
- Louise DACHELET, Cadette stagiaire PEC
- Matthias MAHÉ, PEC
- Aude OLLIVIER CADORET, Région Bretagne

Ainsi qu'à l'équipe communication du Pôle d'excellence cyber :

- Naïké FREMIN DU SARTEL
- Nathan ROLLAND

Cet ouvrage a bénéficié d'une aide de l'État gérée par l'**Agence Nationale de la Recherche** au titre de **France 2030** portant la référence : "ANR-23-CMAS_0026".

FICHE MISSION	THÈME DU STAGE	EXEMPLES DE MISSIONS - BAC+2/3	EXEMPLES DE MISSIONS - BAC+4/5	OBJECTIF RECYF / NIS2	CORRESPONDANCE AVEC LES 42 RECOMMANDATIONS ANSSI
1	Inventorier et mieux connaître son système d'information.	Recenser le matériel informatique : ordinateurs, tablettes, smartphones, imprimantes.	Réaliser des audits des systèmes critiques.	1. Recensement des systèmes d'information	Règle 4 : Identifier les informations et serveurs sensibles et maintenir un schéma du réseau.
		Identifier les accès aux progiciels et droits associés.	Automatiser les inventaires via des scripts (Python, PowerShell).		
		Maintenir une base à jour des utilisateurs et des équipements connectés.	Concevoir un schéma réseau avancé en intégrant la sécurité des équipements sensibles.		
		Vérifier et mettre à jour les schémas réseau (architectures physiques et logiques).	Proposer des recommandations stratégiques sur la gestion des SI.		
2	Élaborer une politique de sécurité des systèmes d'information (PSSI)	Participer à la rédaction de procédures de sécurité (gestion des mots de passe, sauvegardes).	Élaborer une Politique de Sécurité des Systèmes d'Information (PSSI) alignée avec les normes ISO 27001.	2. Cadre de gouvernance de la sécurité numérique	Règle 3 : Maîtriser les risques d'infogérance. Règle 33 : Adopter les politiques de sécurité dédiées aux terminaux mobiles. Règle 34 : Définir une politique de mise à jour des composants des SI Règle 37 : Définir et appliquer une politique de sauvegarde des composants critiques. Règle 39 : Désigner un référent en SSI et le faire connaître auprès du personnel. Règle 40 : Définir une procédure de gestion des incidents de sécurité Règle 42 : Privilégier l'usage de produits et services qualifiés par l'ANSSI.
		Organiser des sessions de sensibilisation pour les employés.	Superviser la mise en œuvre des plans d'action pour corriger les écarts de sécurité.		
		Assister à l'élaboration de rapports sur les écarts de sécurité identifiés.	Définir les responsabilités et processus de gouvernance en matière de cybersécurité.		
3	Gérer les accès et les profils utilisateurs	Maintenir une liste exhaustive des prestataires et fournisseurs informatiques.	Superviser les audits de conformité des prestataires.	3. Maîtrise de l'écosystème	Règle 3 : Maîtriser les risques liés à l'infogérance.
		Vérifier les contrats de prestation pour s'assurer de leur conformité avec les exigences de sécurité.	Élaborer des politiques spécifiques de sécurité pour les relations fournisseurs.		
		Suivre les audits et rapports simples sur les services externalisés.	Proposer des indicateurs pour mesurer la conformité des prestations externalisées.		

4	Gérer les accès et les profils utilisateurs	Créer et gérer les comptes utilisateurs et les droits associés (création, modification, suppression).	Concevoir et implémenter un système de gestion des identités et des accès (IAM).	4. Sécurité et ressources humaines	Règle 2 : Sensibiliser les utilisateurs aux bonnes pratiques. Règle 6 : Organiser les procédures d'arrivée, de départ et de changement de fonction.
		Participer à la sensibilisation des nouveaux employés aux bonnes pratiques de cybersécurité (ex. : formation de base).	Réaliser des audits détaillés des accès et droits utilisateurs.		
		Maintenir une documentation claire des profils utilisateurs et de leurs accès.	Superviser et optimiser les processus d'intégration et de départ des employés en conformité avec les politiques en vigueur.		
5	Maintenir en conditions opérationnelles	Identifier les comptes privilégiés (admin, super-user) et vérifier leurs accès.	Superviser la gestion des mises à jour des systèmes critiques.	5. Maîtrise des systèmes d'information	Règle 5 : Disposer d'un inventaire des comptes privilégiés et le maintenir à jour.
		Appliquer les correctifs de sécurité sur les postes et serveurs.	Automatiser les processus de suivi des vulnérabilités et correctifs via des outils spécialisés.		
		Tester et documenter les processus de sauvegarde et restauration.	Proposer des améliorations pour renforcer la sécurité et la résilience des systèmes critiques.		
		Réaliser des scans de vulnérabilités sur les systèmes critiques.			
6	Contrôler les accès physiques et logiques	- Enregistrer et gérer les accès physiques via des badges, des registres ou des serrures électroniques.	- Concevoir et déployer des systèmes avancés de surveillance des locaux critiques (vidéosurveillance intelligente, biométrie).	6. Maîtrise des accès physiques aux locaux	Règle 26 Protéger et contrôler l'accès aux salles serveurs et locaux techniques.
		- Contrôler l'accès aux salles serveurs et locaux techniques.	- Superviser des audits de sécurité physique pour les installations sensibles.		
		- Installer des dispositifs de vidéosurveillance ou alarmes sous supervision.			

10	Gérer les identités et les accès	- Administrer les droits d'accès pour les utilisateurs, groupes et ressources.	- Mettre en œuvre des politiques avancées d'authentification forte (MFA, biométrie).	10. Gestion des identités et des accès	Règle 8 : Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur Règle 9 : Attribuer les bons droits sur les ressources sensibles du système d'information Règle 12 : Changer les éléments d'authentification par défaut sur les équipements et services Règle 13 : Privilégier lorsque c'est possible une authentification forte Règle 10 : Définir et vérifier des règles de choix et de dimensionnement des mots de passe
		- Configurer et surveiller les règles de mots de passe.	- Auditer et optimiser les mécanismes de gestion des identités et droits à l'échelle de l'organisation.		
		- Documenter les changements dans les accès et les droits.	- Superviser les accès administrateurs et les mécanismes de traçabilité.		
11	Sécuriser l'administration des systèmes d'information	- Configurer les postes d'administration en appliquant les bonnes pratiques de sécurité.	- Déployer des infrastructures dédiées et sécurisées pour l'administration.	11. Maîtrise de l'administration des systèmes d'information	Règle 11 : Sécuriser l'administration et les accès privilégiés. Règle 27 : Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du SI. Règle 28 : Utiliser un réseau dédié et cloisonné pour l'administration du SI. Règle 29 : Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail.
		- Vérifier les accès des comptes administrateurs.	- Élaborer un système de journalisation avancé pour tracer les activités des administrateurs.		
		- Gérer les configurations des dispositifs de sécurité.	- Mener des audits réguliers des accès administrateurs et des systèmes critiques.		
		Configurer la supervision des accès administrateurs et des mécanismes de traçabilité			
12	Identifier et réagir aux incidents de sécurité	Collecter et Analyser les logs pour détecter les anomalies au moyen d'outils automatisés (SIEM)	- Coordonner une cellule de crise en cas d'incidents majeurs.	12. Identification et réaction aux incidents de sécurité	Règle 36 : Activer et configurer les journaux des composants les plus importants. Règle 40 : Définir une procédure de gestion des incidents de sécurité
		- Appliquer les procédures de réponse aux incidents (ex. : isolement des machines infectées).	- Élaborer des rapports d'incidents et proposer des mesures correctives.		
		- Maintenir une documentation sur les incidents survenus.	- Mettre en place un système d'amélioration continue basé sur l'analyse des incidents récurrents.		

13	Garantir la continuité et la reprise d'activité	- Tester les plans de sauvegarde et de restauration.	- Élaborer et tester des plans de continuité et reprise d'activité (PCA/PRA).	13. Continuité et reprise d'activité	Règle 37 : Définir et appliquer une politique de sauvegarde des composants critiques
		- Participer à la mise à jour des logiciels et systèmes.	- Identifier les systèmes critiques à prioriser pour une reprise rapide après sinistre.		
		- Documenter les procédures de reprise après sinistre.	- Superviser les tests des plans de reprise avec des scénarios réalistes.		
		Participer à l'élaboration des PCA/PRA			
14	Piloter la réaction aux crises d'origine cyber	- Participer à la mise en œuvre de plans d'urgence.	- Coordonner la réponse aux crises cyber.	14. Réaction aux crises d'origine cyber	
		- Suivre l'application des mesures post-crise.	- Élaborer des rapports stratégiques pour les directions.		
			- Superviser des exercices de simulation de crise.		
15	Organiser des exercices, tests et entraînements de cybersécurité	- Participer à des exercices de simulation d'incidents.	- Concevoir et diriger des scénarios d'exercices de simulation cyber.	15. Exercices, tests et entraînements	Règle 37 : Définir et appliquer une politique de sauvegarde des composants critiques
		- Documenter les résultats des tests et entraînements.	- Évaluer les performances des équipes de réponse lors des tests.		
		- Appliquer les protocoles de tests sous supervision.	- Identifier les améliorations possibles à intégrer dans les processus après chaque simulation.		
16	Piloter une approche par les risques	Contribuer à l'évaluation des risques de non-conformité réglementaire (NIS, RGPD, Dora).	Réaliser des analyses de risques avancées (méthode EBIOS, ISO 27005).	16. Approche par les risques	Règle 41 : Mener une analyse de risques formelle.
		Maintenir à jour une documentation des risques identifiés.	Mettre en place un plan d'atténuation des risques.		
		Participer à des analyses de risques simples sous supervision.	Élaborer des matrices de risques et des tableaux de bord pour la direction.		

17	Auditer la sécurité des systèmes d'information	Effectuer des scans de vulnérabilités sur le réseau.	Réaliser des audits avancés (évaluation de conformité avec ISO 27001).	17. Audit de la sécurité des systèmes d'information	Règle 17 : Superviser, auditer et documenter la sécurité. Règle 38 : Procéder à des contrôles et audits de sécurité réguliers, puis appliquer les actions correctives.
		Compiler et documenter les résultats des audits sous supervision.	Superviser des campagnes de tests d'intrusion (pentests).		
		Participer à l'analyse des failles de sécurité identifiées.	Établir des recommandations stratégiques basées sur les résultats des audits.		
		Identifier et évaluer les non conformité réglementaires			
18	Sécuriser les configurations des systèmes d'information	- Configurer les postes de travail selon les bonnes pratiques.	- Élaborer des guides de configuration sécurisée pour les systèmes.	18. Sécurisation des configurations	Règle 14 : Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique (durcissement, limitation des logiciels installés) Règle 16 : Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité
		- Désactiver les configurations par défaut dangereuses.	- Superviser les mises en œuvre de configurations avancées.		
		- Tester les configurations des systèmes avant mise en production	- Auditer les configurations existantes et proposer des correctifs adaptés.		
		Superviser l'intégrité des fichiers de configuration de sécurité			
19	Administrer les systèmes d'information depuis des ressources dédiées	- Configurer les postes d'administration.	- Déployer des infrastructures dédiées à l'administration sécurisée.	19. Administration des SI depuis des ressources dédiées	Règle 8 : Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur Règle 27 : Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information Règle 28 : Utiliser un réseau dédié et cloisonné pour l'administration du système d'information
		- Suivre les accès aux systèmes d'administration.	- Implémenter des protocoles sécurisés pour l'administration à distance.		
		- Appliquer les bonnes pratiques pour sécuriser les réseaux d'administration.	- Superviser les audits des activités liées à l'administration.		
20	Superviser la sécurité des systèmes d'information	- Utiliser les outils de supervision pour surveiller les événements de sécurité.	- Mettre en place des solutions avancées de supervision (SIEM).	20. Supervision de la sécurité des SI	Règle 36 : Activer et configurer les journaux des composants les plus importants

POUR ALLER PLUS LOIN

Pour approfondir les sujets abordés dans ce guide, plusieurs ressources permettent d'identifier les formations disponibles, de mieux comprendre les dispositifs liés à l'alternance ou aux stages.

Se former et identifier les compétences cyber

Catalogue des formations cyber en Bretagne
Un panorama des formations proposées sur le territoire breton, du niveau technicien aux cursus spécialisés.

Cartographie des certifications et compétences cyber en Bretagne
Une cartographie interactive permettant de visualiser l'offre de formation et de certification sur le territoire.

GREF Bretagne - Offre de formation
Le portail régional de référence pour rechercher une formation, notamment en apprentissage.

Bretagne Alternance
Une plateforme dédiée à l'apprentissage et à l'alternance en Bretagne.

Comprendre et préparer l'alternance

Ministère du Travail et des solidarités - Apprentissage
Informations de référence sur le contrat d'apprentissage, les conditions d'accès, les obligations des employeurs et les dispositifs d'aide.

DREETS Bretagne - Alternance et apprentissage
Les informations réglementaires et dispositifs applicables en Bretagne.

France compétences - Référentiels et niveaux de prise en charge
Les bases de données permettant notamment de consulter les certifications professionnelles et les niveaux de financement associés aux contrats d'apprentissage.

La Bonne Alternance - Simulateur de rémunération
Un outil permettant d'estimer la rémunération d'un alternant dans le secteur privé.

CNFPT - L'apprentissage dans les collectivités territoriales
Les principales informations destinées aux collectivités souhaitant recruter et accompagner un apprenti.

OPCO Atlas - Financement de l'alternance
Informations relatives aux niveaux de prise en charge des contrats d'apprentissage et aux aides mobilisables par les employeurs.

OPCO Atlas - Guide du tutorat

Conseils pratiques pour organiser l'accueil, l'accompagnement et le suivi d'un alternant au sein de l'entreprise.

Trouver une alternance

La Bonne Alternance

Un service public permettant de rechercher des offres d'emploi en alternance et d'identifier des entreprises susceptibles de recruter.

Comprendre la réglementation cyber

MonEspaceNIS2 - ANSSI

Un service permettant aux organisations d'évaluer leur situation au regard de NIS 2 et d'accéder aux principales exigences applicables.

ANSSI - Guide d'hygiène informatique

Un ensemble de mesures essentielles destinées à renforcer la sécurité des systèmes d'information.

Décrypter le vocabulaire de la cybersécurité

CyberDico - ANSSI

Un dictionnaire permettant de retrouver les définitions des principaux termes utilisés en cybersécurité.

Glossaire Cyber

Une ressource complémentaire pour mieux comprendre les notions techniques et les acronymes du secteur.

NOTES

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org