RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

pix

Référentiel

Les compétences numériques en cybersécurité sur Pix

Accompagner le développement des compétences numériques pour la sécurité de tous

Version 1.0 - Janvier 2025

Avant-propos

Près de 6 entreprises sur 10 estiment que la cybersécurité nécessite un engagement majeur ou se sentent insuffisamment protégées[1]. Face à ces défis, Pix et ses partenaires ont conçu un référentiel complémentaire dédié à la cybersécurité, Pix+ Cybersécurité, qui permet d'évaluer des compétences numériques spécifiques en matière de cybersécurité.

Le référentiel Pix+ Cybersécurité complète le référentiel Pix, format opérationnel du cadre de référence des compétences numériques (CRCN), inspiré du cadre européen (DigComp).

Une réponse à des besoins multiples

Adapté aux élèves dès la cinquième, étudiants, professionnels, et demandeurs d'emploi, ce référentiel se veut un outil pédagogique de référence pour les enseignants et formateurs. Il met l'accent sur les fondamentaux nécessaires pour sécuriser les usages numériques, tant personnels que professionnels.

Il offre également des bases solides pour initier ou renforcer des parcours vers les métiers de la cybersécurité, répondant ainsi à la demande croissante de profils qualifiés dans ce domaine stratégique. Il ne s'adresse pas aux professionnels et experts de la cybersécurité.

[1] *Source : Memento de cybersécurité à l'attention des dirigeants de TPE-PME - Cybermalveillance.gouv.fr.*

Deux approches complémentaires :

1 Les compétences transverses en cybersécurité dans le référentiel Pix

Cette première partie s'inscrit dans les compétences « 4.1. Sécuriser l'environnement numérique » et « 4.2. Protéger l'environnement numérique » du référentiel Pix. Elle couvre les bases essentielles : bonnes pratiques, comportements prudents et utilisation d'outils de sécurité.

Pix s'est associé à l'ANSSI, référence française en matière de cybersécurité, et à Cybermalveillance.gouv.fr pour co-concevoir des outils pédagogiques adaptés à tous les niveaux, du débutant au confirmé. Ce partenariat d'expertise a permis de développer des contenus innovants et des défis ludiques sur la sécurité numérique, accessibles à tous sur Pix.

Les compétences numériques en cybersécurité abordées dans cette première partie s'appuient sur le Cadre de référence européen DigComp. Elles sont utiles à tous (élèves, étudiants, professionnels, demandeurs d'emploi, retraités...) et adaptées à toutes situations, indépendamment des outils ou logiciels utilisés.

2 Les compétences Pix+ Cybersécurité

Pix+ Cybersécurité enrichit le référentiel existant en renforçant les compétences nécessaires au pilotage, à l'anticipation, à la détection et à la gestion des risques cyber dans les organisations, et en sensibilisant aux différents métiers de la cybersécurité pour les rendre encore plus attractifs. Ce référentiel additionnel permet d'évaluer des compétences complémentaires en cybersécurité, d'orienter vers des formations adaptées et de valoriser les acquis.

pix+ Cybersécurité

Il s'adresse à des publics variés.

- Pour les élèves et étudiants, il permet de mieux comprendre le secteur de la cybersécurité, ses métiers et ses acteurs, tout en développant une culture générale sur un domaine en pleine expansion.
- Pour les professionnels, Pix+ Cybersécurité accompagne leur montée en compétences en leur permettant de mieux appréhender et gérer les risques cyber, avec une attention particulière pour les formateurs qui souhaitent sensibiliser leur structure.

Le projet Pix+ Cybersécurité est développé dans le cadre du programme « Talents Cyber » piloté par le Campus Cyber, avec la participation d'un consortium de 13 membres (universités, organismes publics et privés, associations, fondations).

CAMPUS CYBER · Université Sorbonne Paris Nord · Université Paris 1 Panthéon Sorbonne · CY Cergy Paris Université · CNED · Académie de Versailles (Liberté Égalité Fraternité) · Fondation CGénial · Women 4 Cyber (European Cyber Security Organisation) · RootMe Pro · onisep · Class'Code · radiofrance

Ce travail a bénéficié d'une aide de l'État gérée par l'Agence nationale de la Recherche au titre de France 2030.

Sommaire

Les compétences en cybersécurité sur la plateforme Pix 6

Sécuriser l'environnement numérique 7

Protéger les données personnelles et la vie privée 8

Connaître les concepts de la cybersécurité et son écosystème 9

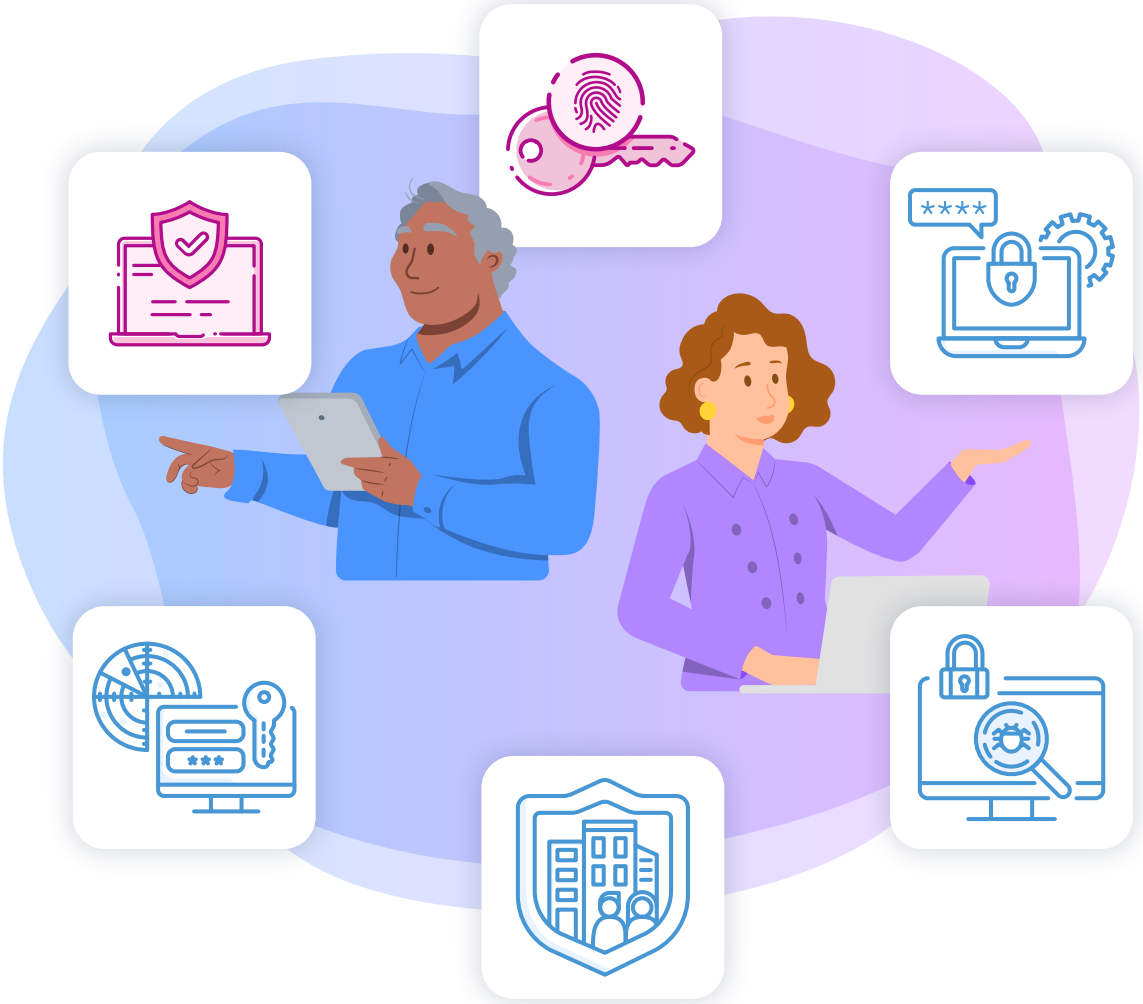
Anticiper les attaques pour protéger les activités d'une organisation 10

Protéger une organisation 11

Détecter et réagir aux incidents 11

Contacts 12

Les compétences en cybersécurité sur la plateforme Pix



Sécuriser l'environnement numérique*

Les thématiques :

- Identification et réaction face aux principales menaces
- Authentification sécurisée
- Utilisation d'Internet en sécurité
- Protection des équipements informatiques

Menaces
Connaître les principales menaces (dont les logiciels malveillants)

Technique de piraterie
Connaître différentes techniques de piraterie informatique et leurs auteurs

Sources d'infection
Connaître les pratiques susceptibles d'infecter un ordinateur

Techniques de manipulation
Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique)

Hameçonnage
Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique)

Robustesse des mots de passe
Connaître les recommandations pour le choix d'un mot de passe robuste

Bonnes pratiques relatives aux mots de passe
Connaître les bonnes pratiques liées à la sécurisation des mots de passe face aux risques de dévoilement

Double authentification
Connaître l'intérêt, le fonctionnement et les limites de la double-authentification

Paiement
Réaliser des paiements de manière sécurisée

Chiffrement des communications
Connaître les apports et le fonctionnement du chiffrement des communications

Wifi sécurisé
Identifier un réseau wifi sécurisé et connaître son principe de fonctionnement

Sécurité d'un site web
Identifier une connexion web sécurisée et connaître le principe de fonctionnement du protocole HTTPS

Cloud
Être sensibilisé à la sécurité du stockage sur le cloud et sur les data center

Outils de prévention et protection
Connaître les logiciels de protection des équipements informatiques

Utiliser un antivirus
Connaître le rôle d'un antivirus et les bases de son utilisation

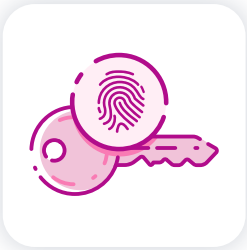
Installation sûre d'un logiciel
Maîtriser les étapes d'installation d'un logiciel en toute sécurité

Logiciel et faille
Etre sensibilisé à la sécurité du système d'exploitation et de ses failles (mise à jour, faille)

Accès aux équipements
Protéger l'accès aux équipements physiques

Verrouillage de session
Connaître le verrouillage de session et ses bonnes pratiques

**Les compétences signalées en rose font parties des compétences transversales Pix, disponibles sur la plateforme dans le grand domaine «Protection et sécurité».*



Protéger les données personnelles et la vie privée

Les thématiques :

- Diffusion volontaire de ses données personnelles
- Collecte de ses données personnelles
- Traces numériques

CGU et politique d'utilisation des données

Localiser, lire et comprendre les conditions générales d'utilisation d'un service en ligne et sa politique d'utilisation des données

Diffusion de données personnelles

Identifier les situations pouvant entraîner la diffusion publique de ses données personnelles

RGPD

Connaître les éléments clé de la protection des données personnelles dans le monde (autorité de protection, extra-territorialité du RGPD, règles de transfert)

Protection des données personnelles dans le monde

Connaître les principes clé de la législation européenne en matière de protection de données personnelles (objectif, droits, limites)

Publicités et lettres d'information

Contrôler la réception d'offres promotionnelles et de lettres d'information

Données personnelles

Connaître les notions de données à caractère personnel, de recoupement et d'anonymisation

Accès d'une application aux données

Maîtriser l'accès à ses données lors de l'installation d'une application

Adresse IP

Connaître l'adresse IP comme trace de connexion identifiante

Traces de connexion

Connaître la nature et la localisation des traces laissées lors d'une connexion internet et savoir les effacer (historique de navigation, cookies, etc)

Localisation d'une adresse IP

Connaître et utiliser la capacité du GPS et d'une adresse IP à géolocaliser un appareil

Connaître les concepts de la cybersécurité et son écosystème*

Les thématiques :

- Connaître les grands concepts de la cybersécurité
- Connaître l'écosystème de la cybersécurité

Vocabulaire et modèles théoriques

Identifier le vocabulaire principal et les manières de penser la cybersécurité

Cadre légal

Connaître le cadre légal et les sanctions associées au piratage

Cryptographie

Appréhender les notions de bases de la cryptographie

Métiers de la cybersécurité

Identifier les principaux métiers technique de la cybersécurité

Enjeux de la cybersécurité

Identifier les principaux acteurs de la cybersécurité nationaux et internationaux

Géopolitique

Identifier les principaux enjeux géopolitiques liés à la cybersécurité

**Les compétences signalées en bleu font parties des compétences complémentaires Pix+ Cybersécurité.*

Anticiper les attaques pour protéger les activités d'une organisation

Les thématiques :

- Anticiper les attaques
- Anticiper la sécurité des données
- Mettre en place des procédures et des contrôles

Analyse de risques

Identifier et analyser les risques de cybersécurité pour une organisation

Chemins de compromissions

Identifier et limiter les chemins de compromission

Confidentialité des données

Maîtriser la diffusion des données

Cartographie des traitements de données personnelles

Cartographier les données personnelles dans une organisation

Traçabilité et journalisation

Comprendre les bases de la journalisation et de la traçabilité

Connaissances juridiques

Identifier les principes clé de la législation européenne
en matière de cybersécurité

PSSI

Comprendre les enjeux d'une politique de sécurité du système d'information (PSSI)

PCA / PRA

Organiser la résilience de l'organisation

Audit et contrôle

Connaître les typologies d'audit et de contrôle et leurs rôles

Protéger une organisation

Les thématiques :

- Protéger grâce à des bonnes pratiques
- Protéger techniquement

Séparation des usages

Séparer les usages personnels et professionnels

Nomadisme

Limiter les risques du nomadisme

Sécurité physique des appareils numériques

Sécuriser l'accès physique aux équipements

Réseaux et architecture d'un système d'information

Sécuriser les réseaux d'une organisation

Logiciel

Sécuriser les logiciels utilisés dans une organisation

Outils de protection

Connaître les différents outils de protections dans une organisation, leurs rôles, leurs fonctionnalités , leurs limites et où les installer

Détecter et réagir aux incidents

Les thématiques :

- Détecter une cyberattaque
- Réagir à un incident

Détection d'une cyberattaque

Signaler et détecter les événement suspects dans une organisation

Violation de données personnelles

Identifier et réagir à une violation de données personnelles

Communication de crise

Communiquer de manière adaptée en cas de crise

Investigation numérique (forensique)

Être sensibilisé à l'investigation numérique (forensic)

Cellule de crise

Connaître le fonctionnement d'une cellule de crise

Cycle de réponses aux incidents

Comprendre le cycle de réponses aux incidents

Contacts

Une question sur nos compétences numériques en cybersécurité ou un projet à destination de vos apprenants ? **Contactez-nous :**

pix.fr/cybersecurite