Version 4.12 | 28/08/2025

Qui sommes-nous ?

Public

2019

Création

14

Collaborateurs

5000

Emplois cyberprotégés

85

Clients

Prestataire Breton

Une société fondée sur 3 valeurs

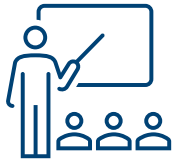
Déontologie

Aucun partenariat avec des éditeurs ou intégrateurs de solutions pour préserver notre indépendance

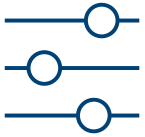
Chacun de nos clients est différent, la solution l'est aussi pour qu'elle soit efficace

Ambassadeur des règles de la cybersécurité, que nous appliquons chez nos clients

Accessibilité



Explications claires et à la hauteur du public visé



Ambitions, coûts associés et capacités adaptées aux PME, ETI et collectivités territoriales

R&D pour adapter les procédés des grandes entreprises aux plus petites

Engagement

Compétences en cybersécurité partagées auprès de divers acteurs pour faire bouger les choses

10 jours par an imposés à nos collaborateurs pour des missions d'intérêt général en cybersécurité (enseignement, réserve, engagement associatif, etc.)

Nos certifications, qualifications et engagements

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Labellisé depuis 2020

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE
La certification a été délivrée au titre de la catégorie d'action suivante :
Actions de formation

Certifié en 2023

ACTEUR de BREIZHFAB
L'INDUSTRIE AMBITIEUSE

Depuis 2020 :
Prestataire référencé en cybersécurité

VISA DE SÉCURITÉ
ANSSI

Depuis 2025 :
Qualification PASSI en cours

Breizh Cyber

Prestataire référencé en réponse à incident

Membre fondateur
Bretagne Cyber Alliance

Référencé Expert Cyber

Engagés pour notre territoire, nous enseignons dans les écoles :

UIMM – PÔLE FORMATION – LA FABRIQUE DE L'AVENIR

ESNA de Bretagne – École Supérieure du Numérique Appliqué – orange™

GRC*
Gestion de crise

IEQT – L'École du management des risques et de la performance

Référent Cyber

esli – ÉCOLE SUPÉRIEURE DE LOGISTIQUE INDUSTRIELLE – CAMPUS E.S.P.R.I.T. Industries – GROUPEMENT D'INTÉRÊT PUBLIC

Sécurité des
systèmes industriels

SUP DE VINCI – INGÉNIERIE DES SYSTÈMES D'INFORMATION

Supervision des SI*
PKI*
Continuité d'Activité

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
Liberté
Égalité
Fraternité

Université Bretagne Sud – ubs – Gendarmerie nationale – Une force humaine

GRC*

École d'ingénieurs – ensibs – Université Bretagne Sud

GRC*
Supervision des SI*
Reverse*

UNIVERSITÉ DE RENNES 1

Sécurité des
systèmes industriels

l'X – ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

GRC*

La garantie pour nos clients de disposer d'ingénieurs pédagogues et suivant les meilleures pratiques !

GRC : Gouvernance, Risques, Conformité. Ce sont l'ensemble des méthodes qui permettent de gérer par des processus et des règles communes la cybersécurité dans une organisation.

SI : Systèmes d'Information. Ce sont des systèmes comprenant l'ensemble de vos données et équipements informatiques. Ils ont pour objet d'opérer des traitements sur vos données.

PKI : « Public Key Infrastructure » ou Infrastructure de Gestion de Clés. Infrastructures permettant de gérer des clés cryptographiques et/ou des certificats en vue de faire du chiffrement, de l'authentification, etc.

Reverse : discipline permettant de comprendre le fonctionnement d'un logiciel (et ses potentielles vulnérabilités) sans disposer du code source de ce même logiciel.

Que signifie WALLACK ?

Wallack vient du mot « *wallhack* »

Le mot « *wallhack* » est un terme issu du monde vidéoludique. Il désigne un outil de triche permettant à un joueur de voir ses ennemis à travers les murs.

Pourquoi cette référence ?

Évoluer dans le cyberespace, c'est se frayer un chemin dans une large étendue sans aucune vision

Souvent, nous ne connaissons pas totalement notre propre système d'information

VOUS êtes le joueur et vous évoluez dans un monde où vous ne voyez qu'à proximité immédiate

Dans un jeu, si nous perdons nous recommençons.

Dans la vie, si votre organisation perd, vous ne pourrez pas forcément relancer la partie !

Le contexte des PME/ETI et des collectivités

Des employés seuls dans leur corps de métier

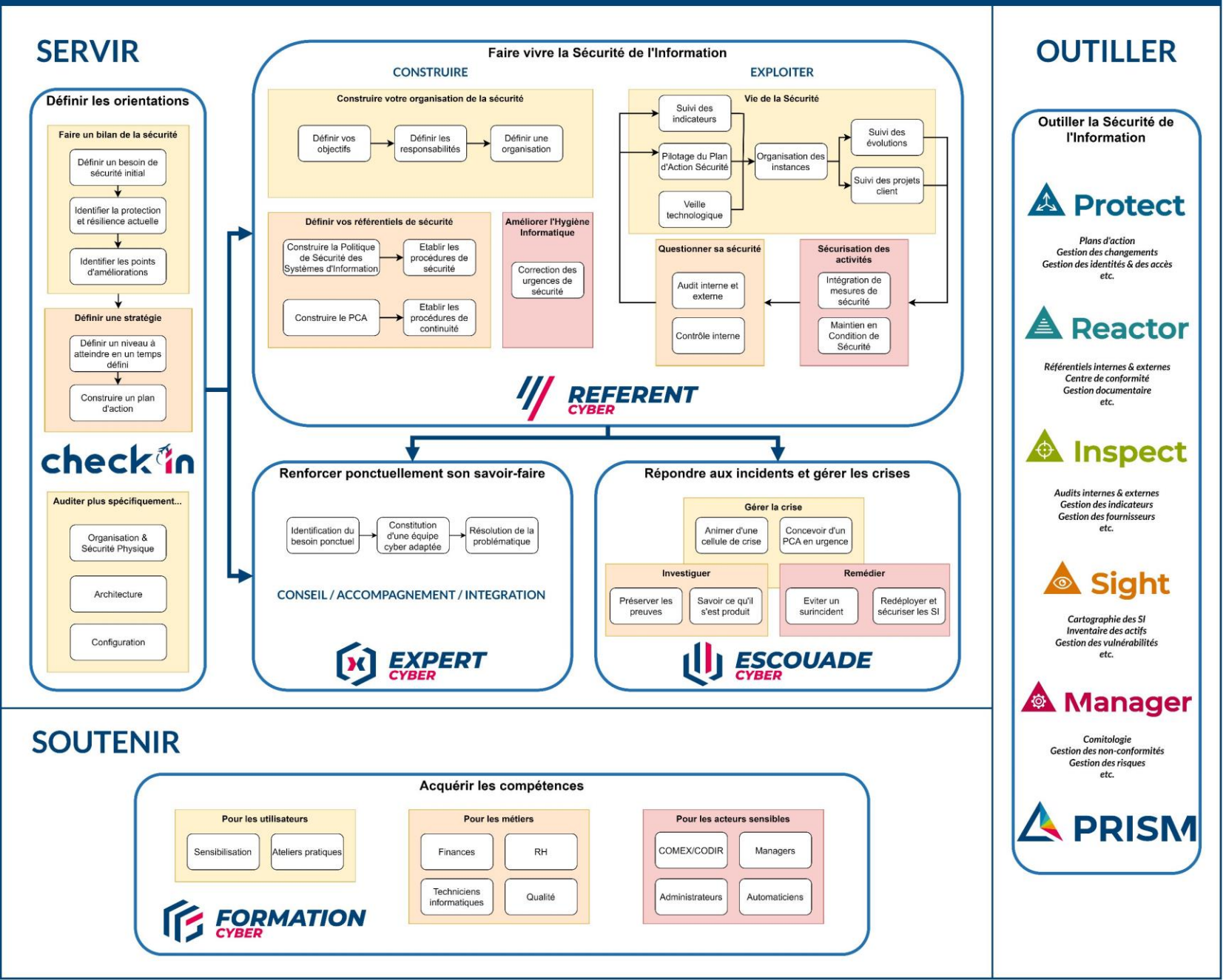
Veille et évolution des compétences difficiles

Loin des grands acteurs de la cybersécurité

Des normes et guides peu adaptés à votre contexte

Comment notre démarche vous permet de vous sécuriser ?

UN CATALOGUE TAILLÉ SELON LE DÉROULEMENT D'UNE DÉMARCHE EN CYBERSÉCURITÉ



Comment notre démarche vous permet de vous sécuriser ?

Nos prestations en détail

check in

Audits

EXPERT CYBER

Expertise à la demande

PRISM

Suite Logicielle dédiée à la Cyber

REFERENT CYBER

Service cyber externalisé

ESCOUADE CYBER

Réponse à incident
Gestion de crise

FORMATION CYBER

Formation Cybersécurité

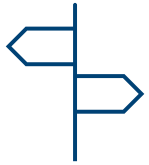
REFERENT CYBER

Votre équipe cybersécurité

Objectif : Incarner le service cybersécurité de votre organisation

Equipe sécurité comptant :

- Un RSSI
- Experts en GRC
- Experts SecOps



Possibilité d'externaliser totalement ou partiellement

Point de contact avec vos équipes informatiques ou vos prestataires externes

*RSSI : **R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation | Expert en GRC : **G**ouvernance, **R**isque, **C**onformité | Expert SecOps : **Séc**urité **Op**érationnelle*

REFERENT CYBER

Votre équipe cybersécurité

1. Définition d'une **stratégie de sécurité** et des **moyens associés**

2. Mise en place de **processus internes** pour gérer la sécurité, **sensibilisation/formation, contrôle interne**

3. **Sécurisation de vos Systèmes d'Information** (sécurité des réseaux, supervision, administration sécurisée)

4. En cas de **besoin exceptionnel**, profitez d'une **équipe pluridisciplinaire** pour disposer toujours des **meilleures compétences** sur le sujet

EXPERT CYBER

Expertise à la demande

Pour répondre à un besoin ponctuel, de compétence, de réduction des coûts d'un projet ou d'accélérer sa mise en œuvre, notre prestation "Expert Cyber" est là pour vous accompagner. Nous travaillons en étroite collaboration avec votre équipe pour comprendre vos objectifs et déployer les solutions les plus adaptées à vos besoins.

Nos experts en cybersécurité sont hautement qualifiés, titulaires d'un diplôme d'ingénieur en cyberdéfense, avec une expertise avérée à la fois en Gouvernance, Risque, Conformité (GRC) et en Sécurité Opérationnelle (SecOps).

Exemples de réalisations :

- Rédaction de PSSI
- Définition de process et de politiques de sécurité
- Cloisonnement réseau
- Sécurité de l'AD et de l'Administration
- Exercices de gestion de crise
- Plan de Continuité d'Activité et de Reprise d'Activité
- Bilan d'Impact sur l'activité
- Analyse des risques

check in 360°

Audit de maturité

Objectifs :

- Evaluer la maturité cyber d'une organisation en matière de gouvernance, appréciation des risques, conformité et mesures techniques
- Identifier une stratégie de sécurité pragmatique, construire une feuille de route et évaluer les budgets associés

EBIOS RISK MANAGER

Basé sur
EBIOS Risk Manager

Référentiels spécifiques selon
les secteurs d'activités

Audit de maturité rapide et
complet

Nos prestations en détail

check in 360°

1

Définir votre contexte

La définition de votre contexte est l'étape la plus importante.

Elle nous permet de comprendre qui vous êtes, comment vous travaillez, quels sont vos objectifs, quels sont vos points critiques.

Nous pouvons ensuite mieux répondre aux problématiques de sécurité concernant le coeur de vos métiers.

2

Déterminer votre situation

Nous allons dérouler un questionnaire pour connaître votre maturité en cybersécurité.

Une étape clé pour que nous ayons une vision précise de l'existant sur le terrain.

Cela nous permettra de déterminer les aspects à maintenir, à améliorer ou à mettre en place.

3

Création de votre feuille de route

Nous rédigeons votre feuille de route en vous précisant toutes les mesures à mettre en place.

Nous vous conseillons également sur l'amélioration de l'existant et le maintien de votre sécurité.

Chaque mesure sera priorisée et affectée à un service de votre structure pour vous guider dans le déploiement.

4

Vous former à la stratégie

Afin que vous puissiez prendre des décisions en autonomie, nous vous formerons à la stratégie en cybersécurité.

Cette formation est essentielle pour mettre en place votre gouvernance de la sécurité.

Vous pourrez ainsi piloter votre feuille de route et arbitrer les orientations et moyens à mettre en oeuvre.

5

Plan d'actions

Il s'agit de mettre en oeuvre des mesures de sécurité parmi nos recommandations.

Certaines sont complexes à concevoir ou déployer, d'autres le sont moins.

Il vous manque des compétences ?

Des solutions de Wallack ou d'un de nos partenaires peuvent vous être proposées !

Nos audits spécifiques

check in GOUV

Objectif :

Evaluer le niveau de conformité et/ou de sécurité :

- De la gouvernance
- Des politiques
- Des procédures de sécurité

Garantir le maintien en conditions de sécurité du système d'information audité

check in ARCHI

Objectif :

Evaluer le niveau de conformité et/ou de sécurité d'un système d'information notamment par l'analyse :

- Des choix de positionnement des dispositifs matériels et logiciels
- Des interconnexions du système d'information avec des réseaux tiers, en particulier Internet.

check in CONFIG

Objectif :

Evaluer le niveau de conformité et/ou de sécurité de la configuration des dispositifs matériels et logiciels d'un système d'information.

Il peut s'agir par exemple d'équipements réseau, de systèmes d'exploitation, d'applications ou de produits de sécurité

ESCOUADE CYBER

Votre équipe de réponse à incident

Objectif : Gérer une crise en limitant les conséquences

Investigation numérique

Gestion de la crise avec vos équipes

Aide la reconstruction de votre système d'information

ESCOUADE CYBER

Votre équipe de réponse à incident

1. Collecte des preuves et analyse de l'attaque

2. Vous aider dans la gestion de la crise en s'intégrant à la direction pour assister la définition des communications à réaliser ou des actions à mener

3. Création et mise en œuvre d'un plan de reprise d'activité

4. Reconstruction d'un système d'information sain avec les bonnes recommandations de sécurité

FORMATION CYBER

Votre organisme de formation

1. Définition du **cahier des charges** de votre formation
2. **Création sur-mesure** si nécessaire
3. **Accompagnement pédagogique** tout au long de la formation
4. **Ateliers pratiques** et **démonstrations**

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

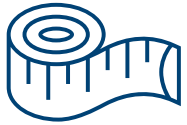
La certification a été délivrée au titre de la catégorie d'action suivante :
Actions de formation

FORMATION CYBER

Votre organisme de formation

Objectif : Former et informer les collaborateurs de votre organisation sur la cybersécurité

Formateurs/trices experts
dans leurs domaines



Formations sur mesure
sans frais supplémentaires

Formations en présentiel
ou en ligne

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE
La certification a été délivrée au titre
de la catégorie d'action suivante :
Actions de formation

PRISM

Suite Logicielle dédiée à la Cybersécurité

Objectif : Assurer la gestion de votre SMSI avec une suite logicielle conçue pour tous les types d'organisations

Gestion de votre SMSI :

- Comitologie
- Plan d'actions
- Intervention et comptes-rendus
- Contrôles et audits

Echange de documents avec vos correspondants Wallack

Cartographie de votre système d'information en temps réel

Gestion dynamique de vos vulnérabilités

SMSI : Système de Management des Sécurité de l'Information

Gardons le contact

✉ contact@wallack.fr
☎ 02.99.22.02.85

✉ youen.heritier@wallack.fr
☎ 07.63.71.31.97