XCELLENS PARTNERS

OFFRE DE SERVICE

EXCELLENS CYBERSECURITY

« Une démarche d'excellence au cœur des problématiques de cybersécurité »

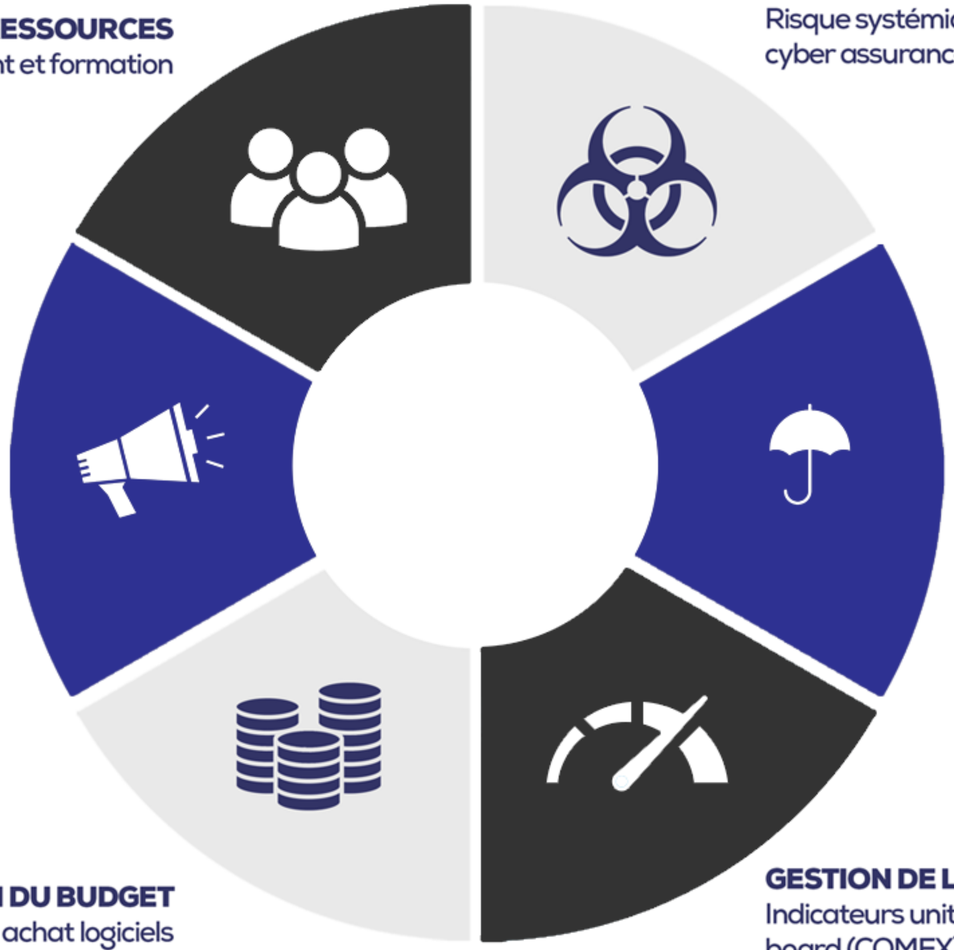
XCELLENS PARTNERS, 1 RUE DE STOCKHOLM 75008 PARIS

I.

II.

LES ENJEUX MANAGÉRIAUX DE LA CYBERSÉCURITÉ

1 - Accompagner les managers dans la gestion des enjeux associés aux problématiques Cybersécurité en proposant une offre de service complète.



GESTION DES RESSOURCES
Recrutement et formation

GESTION DE LA CYBERPROTECTION
Risque systémique et intérêt limité de la cyber assurance

GESTION DE LA COMMUNICATION
Utilisateurs, experts et dirigeants

GESTION DE LA CYBERDÉFENSE
Qualification des impacts en cas d'incident et organisation des actions défensives (SOC, PCA/PRA)

GESTION DU BUDGET
Capacité J/H et coût achat logiciels

GESTION DE LA MESURE
Indicateurs unitaires, management et board (COMEX)

PRÉSENTATION DE NOTRE OFFRE DE SERVICE

1 - Excellens Cybersecurity est une offre de service complète reposant sur une approche TOP – DOWN pour la mise en place d'un dispositif de cybersécurité efficace.

I.

II.

CYBERCOMPLIANCE

- Compréhension de l'organisation de l'entreprise et analyse détaillée de la cyber réglementation entourant l'entreprise
- Cartographie du SI : Applicative et Infrastructure et des Processus afin d'identifier les tâches à risque sur la base du référentiel risques internes
- Mise en place de la cyber compliance au niveau du SI : Adaptation du SI et formation des collaborateurs et de la Direction

▶ **ACCOMPAGNER VOS PROJETS DE CYBER PROTECTION** (risque systémique) et **CYBERDÉFENSE** (qualification des impacts en cas d'incident et organisation des actions défensives (SOC, PCA/PRA)

FORMATION CYBERSÉCURITÉ

- Certification QUALIOPI
- Partenaire académique de qualité : IAE Gustave EIFFEL, ORT Montreuil...
- Ludepedagogie et Serious Game

▶ **SENSIBILISATION ET FORMATION DE VOS COLLABORATEURS, MANAGERS ET DIRECTION GÉNÉRALE.**

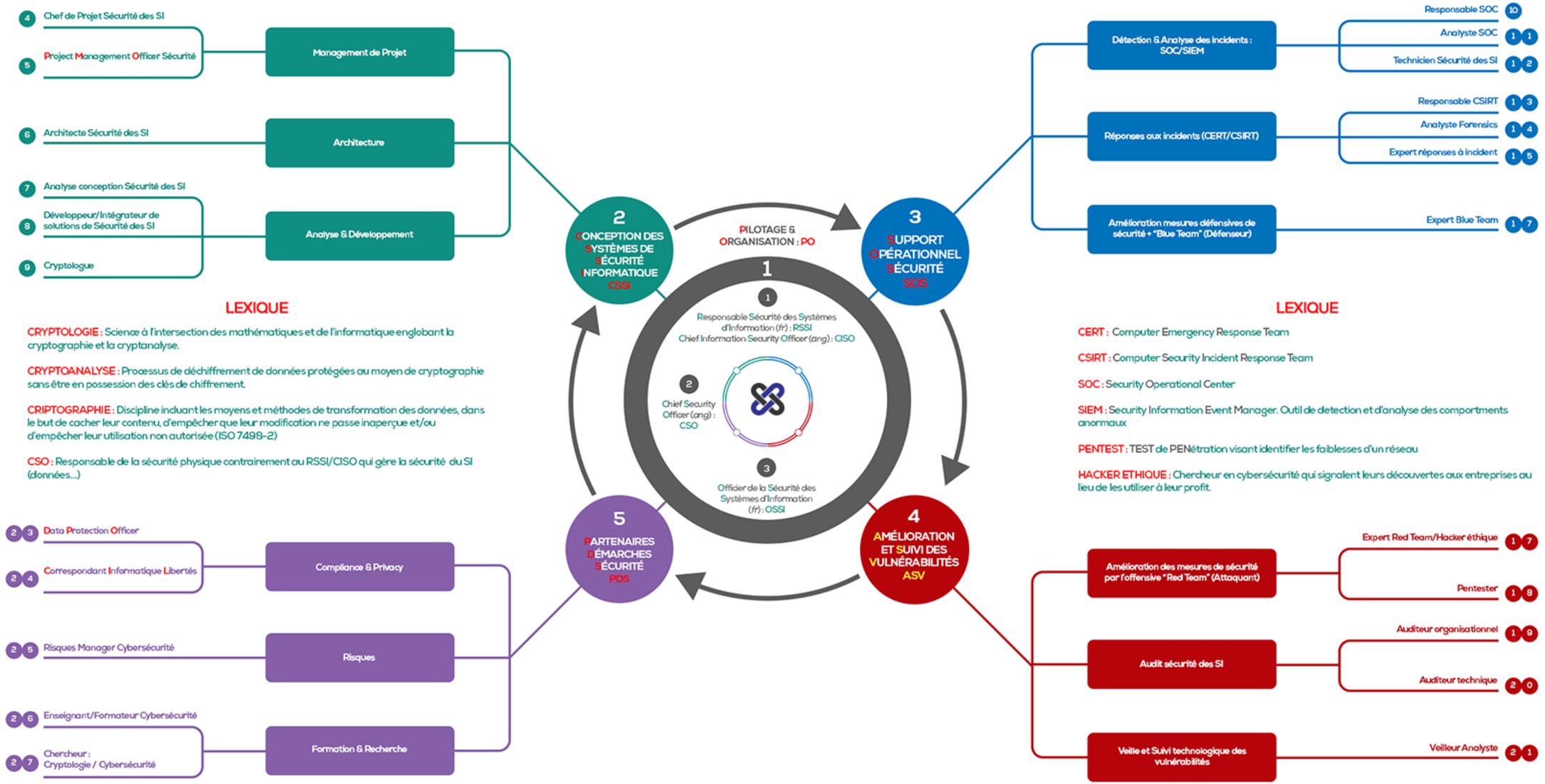
PARTENARIAT ACADÉMIQUE

- Mise à disposition personnalisée de stagiaires et d'alternants
- Améliorer la maturité cyber de votre organisation

▶ **PARTENARIAT AVEC VOS ÉQUIPES OPÉRATIONNELLES POUR PROPOSER DES STAGIAIRES ET ALTERNANTS.**

PRÉSENTATION DE NOTRE OFFRE DE SERVICE

2 - Les profils mis à disposition



LEXIQUE

CRYPTOLOGIE : Science à l'intersection des mathématiques et de l'informatique englobant la cryptographie et la cryptanalyse.

CRYPTOANALYSE : Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.

CRIPTOGRAPHIE : Discipline incluant les moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2)

CSO : Responsable de la sécurité physique contrairement au RSSI/CISO qui gère la sécurité du SI (données...)

LEXIQUE

CERT : Computer Emergency Response Team

CSIRT : Computer Security Incident Response Team

SOC : Security Operational Center

SIEM : Security Information Event Manager. Outil de detection et d'analyse des comportments anormaux

PENTEST : TEST de PENétration visant identifier les faiblesses d'un réseau

HACKER ETHIQUE : Chercheur en cybersécurité qui signalent leurs découvertes aux entreprises au lieu de les utiliser à leur profit.

PRÉSENTATION DE NOTRE OFFRE DE SERVICE

3 - Focus Cartographie du SI : Couche applicative et infrastructure

LES ENJEUX DE LA CARTOGRAPHIE :

- Les enjeux métiers et les activités les plus sensibles pour l'organisation, que ce soit en termes financiers, réglementaires ou d'image. La bonne appréhension des processus clés de l'organisation et l'implication des parties prenantes sont donc des impératifs préalables à toute activité de recensement des risques informatiques.
- Les enjeux en termes de menaces et des évènements redoutés par l'organisation qu'ils soient d'origine interne ou externe. Ces évènements peuvent être classés en deux catégories : les évènements inhérents à la nature même de l'organisation, tels que la dépendance vis-à-vis d'une application clé développée en interne (événements endogènes), et les évènements exogènes comme les attaques virales, les intrusions ou les catastrophes naturelles

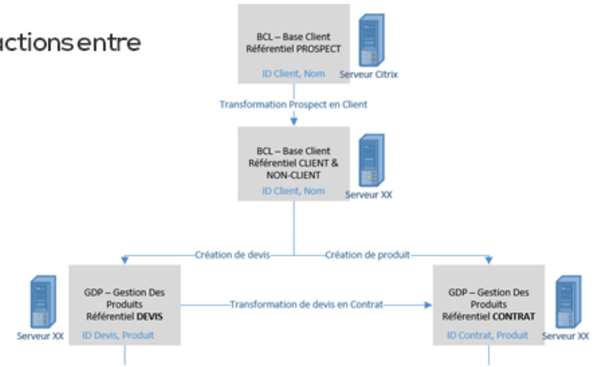
LE CONTENU DE LA CARTOGRAPHIE : Elle est multi-dimensionnel et se décompose en 2 couches. Il s'agit de vues : elles constituent des représentations partielles du système d'information, de ses liens et de son fonctionnement. Elles sont destinées à rendre lisibles et compréhensibles des aspects du système d'information de nature à être exploités par exemple dans les opérations de sécurité numérique.

La Cartographie Applicative : vise à établir un catalogue recensant le patrimoine applicatif de l'entreprise en soulignant les interactions entre applications ou composants d'applications, leur description ainsi que les données échangées.

La Cartographie de l'Infrastructure : Il s'agit de recenser le patrimoine applicatif de l'entreprise en soulignant les interactions entre applications ou composants d'applications, leur description ainsi que l'essentiel des données échangées. Cela se traduit par le recensement :

- des équipements physiques
- des éléments de configuration assurant le fonctionnement du socle technique impératif à toute exécution applicative (définition des plages d'adresses IP, des VLAN et des fonctions de filtrage et routage...)

N.B: MÉTHODOLOGIE UTILISÉE : AUDIT



QUELLE DÉMARCHE ADOPTER ? Une démarche en 4 étapes, dont la mise en œuvre est directement liée d'une part à la nature du système d'information à cartographier, et d'autre part aux objectifs visés par l'organisme selon son niveau de maturité et les enjeux de sécurité numérique.

- Etape n°1 : Définir les enjeux de la cartographie, les acteurs à mobiliser, le périmètre du système d'information à représenter, le niveau de granularité de l'inventaire et les types de vues à réaliser, les différentes étapes d'itération et le calendrier associé.
- Etape n°2 : Définir le modèle de cartographie en ,recensant toutes les informations disponibles en rassemblant les inventaires et schémas de représentation du système d'information déjà constitués. Définir le modèle de représentation de l'inventaire et des différentes vues ainsi qu'une nomenclature pour les différents objets.
- Etape n°3 : Définir l'outillage à utiliser pour la construction de la cartographie et son maintien à jour.
- Etape n°4 : Diffuser et promouvoir la cartographie au sein de l'organisme. Mettre en place un processus de mise à jour et la gouvernance associée

PRÉSENTATION DE NOTRE OFFRE DE SERVICE

4 - Focus sur l'identification des tâches critiques et à risques au niveau des processus métiers

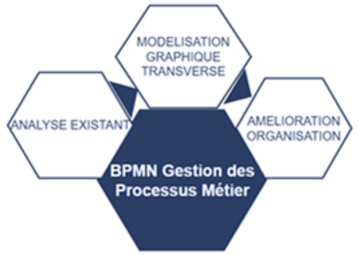
POURQUOI ? Les processus métiers permettent d'avoir une bonne connaissance des échanges d'information et des accès aux systèmes d'information. Le problème est que ces échangent d'information favorisent des risques dont il faut mesurer les impacts et les enjeux. Et l'identification des tâches critiques réalisés par les différents acteurs d'une organisation s'intègre dans une démarche globale de gestion des risques et dé sécurisation du SI.

COMMENT ? Via notre offre BPMN : Gestion des process métiers

Le BPMN permet de partager une même vision des processus au sein de l'organisation. L'objectif est que tous les intervenants, techniques, métier aussi bien que les utilisateurs finaux puissent appréhender facilement les processus de l'organisation
Il s'agit d'un langage commun de modélisation normée est maintenue par OMG (Object Management Group), un consortium américain qui a pour but de standardiser et de promouvoir le modèle objet. Depuis son actualisation en 2011, on parle maintenant de BPMN 2.0 et la norme est devenue le standard incontournable pour la modélisation des processus.

QUELLE EST LA DÉMARCHE DE MODÉLISATION BPMN ? Cette démarche, indépendante de l'outil ou du logiciel BPM utilisé, s'articule autour de 3 axes

- Analyse de l'existant
- Modélisation graphique transverse
- Amélioration de l'organisation :
  - Pilotage par les process
  - Alignement des processus sur la stratégie de l'entreprise

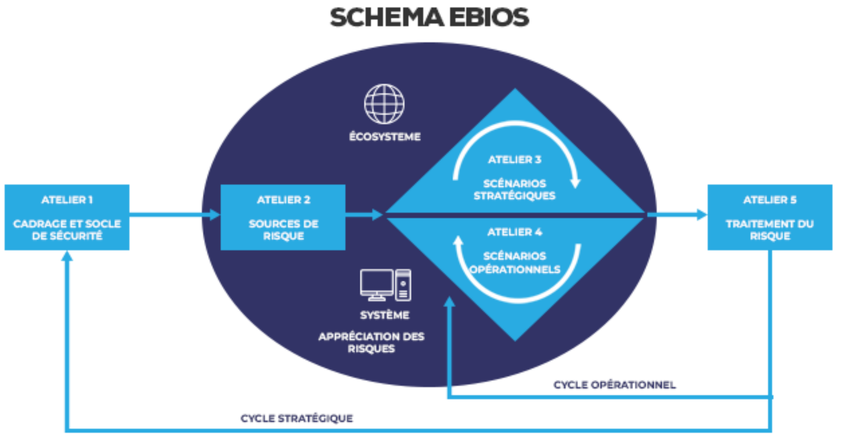


QUELS OUTILS UTILISÉS ? Bizagi, Camunda Modeler

COMMENT DÉTECTER LES TÂCHES CRITIQUES ET À RISQUES DES PROCESS MÉTIERS ?

Utilisation de norme ISO : EBIOS Risk Manager

Utilisation de référentiel MITRE & ATTACK : plateforme qui organise et catégorise divers types de tactiques, techniques et procédures (TTP) utilisées par les acteurs de la menace dans le monde numérique, visant à aider les organisations à identifier les lacunes dans leurs cyberdéfenses.



PRÉSENTATION DE NOTRE OFFRE DE SERVICE

5 - Focus sur quelques exemples de notre démarche cyber compliance

EXEMPLE CYBER COMPLIANCE : CONFORMITÉ RÉGLEMENTAIRE LOI DE PROGRAMMATION MILITAIRE (LPM) DE 2019-2014

Obligations des OIV : Respect des 20 règles LPM répartis en 5 domaines: Gouvernance, Maîtrise des SI, Protection des systèmes, Maîtrise des risques et gestion des incidents (3 mois).

Accompagnement conformité technique (2 ans) : mise en place d'un SOC qualifié PDIS et PRIS (Prestataires de Réponse aux Incidents de Sécurité).

EXEMPLE CYBER COMPLIANCE: CONFORMITÉ RÉGLÉMENTAIRE DIRECTIVE NIS

Obligations des OSE

Accompagnement administratif et analyse :
- Identification de ses systèmes essentiels et déclaration à l'ANSSI
- Analyse d'écarts pour identifier les non-conformités par rapport aux règles de sécurité à mettre en place.

Accompagnement conformité technique :
- Cartographie des SI
- Intégration des solutions de cyber sécurité

Finalisation de la mise en conformité :
- Audit de sécurité des systèmes essentiels ;
- Analyse de risques ;
- Accompagnement à l'homologation.