Offre Valauris
Focus Cyberdéfense.

> **9 sur 10 des entreprises touchées, dont %42 de PME.**

Approche « Top - Down » pour la mise en place d'un dispositif de cybersécurité efficace :

Couche métiers
- Identification des tâches critiques et à risques au niveau des processus métiers

Couche applicative et infrastructures
- Cartographie du SI (Applicative et Infrastructure)

Mise en place dispositifs de cybersécurité
- Mise en place PSSI

La cybersécurité en quelques chiffres

24% PHISHING

20% MALWARE

16% RANÇONGICIEL

42%

1.3M€ LE COÛT MOYEN D'UNE CYBERATTAQUE POUR UNE ENTREPRISE

7 MOIS LE DÉLAI MOYEN D'IDENTIFICATION D'UNE VIOLATION DE DONNÉES

14 SEC LA FRÉQUENCE DES ATTAQUES PAR RANÇONGICIEL DANS LA MONDE

Yvon GATSONO
Consultant Senior

Valauris France

Cell Phone : 06.12.74.00.43
Email : gatsono@yahoo.fr

Axe 1 - Identification les tâches critiques et à risques au niveau des processus métiers

Pourquoi ? 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**.

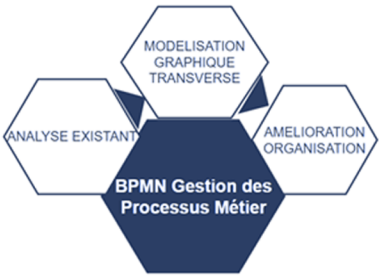
Comment ? Via notre offre BPMN : Gestion des process métiers.

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 maintenue par l'OMG (Object Management Group), qui a pour but de standardiser et de promouvoir le modèle objet. Depuis son actualisation en 2011, le 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

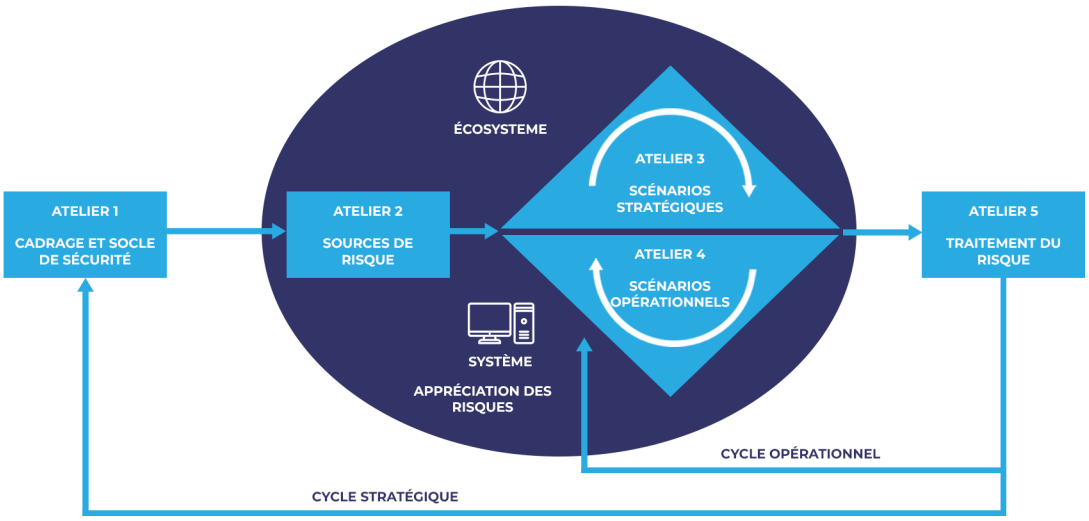


Quels outils utilisés ?

Bizagi, Camunda Modeler

Comment détecter les tâches critiques et à risques des process métiers ?

Utilisation de : EBIOS Risk Manager (basée sur 5 ateliers)



Utilisation du 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 cyberdéfense.

Axe 2 - Cartographie du SI (couche applicative et infrastructure)

Les enjeux de la cartographie :

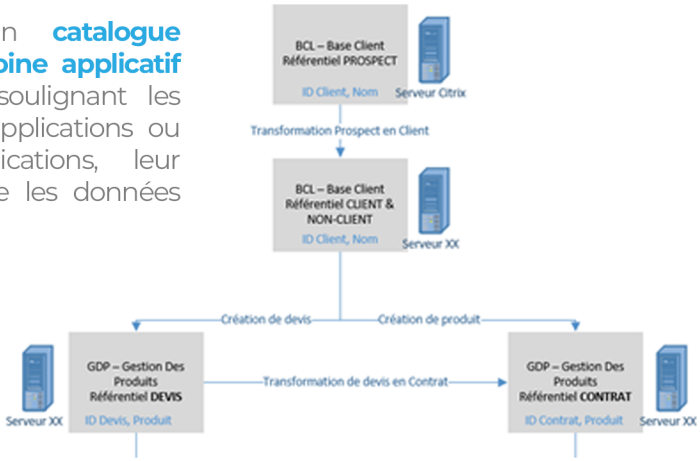
• 1 - Les **enjeux métiers et les activités les plus sensibles pour l'organisation**, que ce soit en termes financiers, réglementaires ou d'image. La bonne appréhension des processus clés de l'organisation et l'implication des parties prenantes sont donc des impératifs préalables à toute activité de recensement des risques informatiques.

• 2 - 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

Les couches de représentation de la cartographie :

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...

Quelle démarche de cartographie adoptée ? 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.

Diagnostic maturité cybersécurité du SI : Eléments de reference

Niveau 0. Pratique inexistante ou incomplète : pratiques de base éventuellement mises en œuvre et le besoin n'est pas reconnu.

Niveau 1. Pratique informelle : pratiques de base mises en œuvre de manière informelle et réactive à l'initiative de ceux qui estiment en avoir besoin.

Niveau 2. Pratique répétable et suivie : pratiques de base mises en œuvre de façon planifiée et suivie, avec un support relatif de l'organisme.

Niveau 3. Processus défini : mise en œuvre d'un processus décrit, adapté à l'organisme, généralisé et bien compris par le management et par les exécutants.

Niveau 4. Processus contrôlé : le processus est coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés.

Niveau 5. Processus continuellement optimisé : l'amélioration des processus est dynamique, institutionnalisée et tient compte de l'évolution du contexte.

Inspiré par l'approche ISO 21827 Cf. Maturité SI. Approche méthodologique. Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil

Axe 3 - Mise en place du dispositif de sécurité

APPROCHE GLOBALE DES ÉLÉMENTS DU DISPOSITIF

Gestion des ressources

• Identification des competences utiles pour la mise en place du dispositif cyber-protection et cyber-defense.

• Mise en place plan de sensibilisation ou de formation

Gestion de la cyber-protection

• Surveiller et anticiper les risques systémiques

• Protéger le SI en anticipant les

Gestion de l'organisation

• KPI et autres indicateurs pour la Direction

• Budget j/h (internes et externes) et coûts logiciels.

• Plan de communication incidents

Gestion de la cyber-résilience

• Mise en place d'un plan de développement general de cyber-resilience

• Plan de Continuité d'Activité (PCA)

• Plan de Reprise d'Activité (PRA)

1ère ligne défense : collaborateurs

Sensibilisation aux risques cybers

• Formation Classique : Powerpoint.
• Usage de la ludopé dagogie : Security Games

2ème ligne de défense : dispositif de protection du SI

Aligner le dispositif sur la maturité de l'entreprise

• PSSI : Normes, procedures...
• Cartographie risques EBIOS RM
• Spécifications fonctionnelles et techniques

3ème ligne de défense : Cyber-assurance

Assurer son SI

• Souscrire un contrat d'assurance adapté à ses besoins.
• Partager le impacts financiers

Vous souhaitez en savoir plus sur notre offre de service, recevoir notre cartographie ou nos modèles de fiches de poste, le responsable de notre offre est à votre disposition :

Yvon GATSONO
Consultant Senior

Valauris France

Cell Phone : 06.12.74.00.43
Email : gatsono@yahoo.fr