Formation Cybersécurité et BPM

Objectifs de la formation Cybersécurité BPM

La transformation numérique, la dématérialisation, les nouveaux usages de communication avec les médias sociaux, la nécessité pour l'entreprise de s'ouvrir toujours plus vers l'extérieur, accentuent de jour en jour l'exposition des entreprises aux cyber-attaques.

La connexion des systèmes d'information avec l'extérieur, la mobilité des salariés et leurs nouvelles applications, augmentent considérablement le risque de failles et de comportements à risque, augmentant la vulnérabilité des entreprises.

Il est donc nécessaire de revoir certaines pratiques de sécurité et d'améliorer le dialogue entre la direction informatique, les métiers et la sécurité. **Le fonctionnement en silos que connaissent la plupart des entreprises, aussi bien en termes de systèmes d'information que d'échanges entre départements ne facilite pas l'approche transverse nécessaire à la sécurité. L'approche processus est un excellent moyen méthodologique pour asseoir des réflexes sécurité dans le quotidien des métiers concernés, en les impliquant de bout-en-bout dans la démarche.**

Toutes les entreprises utilisent des processus pour développer leurs activités, qu'ils soient explicitement écrits ou non. Les processus permettent d'organiser le fonctionnement d'une organisation.
Adopter une vision processus dans une entreprise permet de décrire et d'améliorer son fonctionnement. Les processus peuvent être représentés sur papier ou avec des moyens informatiques via un logiciel de modélisation de processus.

Plus concrètement cette formation Cybersécurité et BPM vous apportera les compétences et connaissances nécessaires pour :

- Découvrir l'impact et l'utilité de la vision processus dans le domaine de la cybersécurité.

- Connaitre l'apport de la discipline BPM (Business Process Management) - ou gestion des processus métier -, dans la sécurisation des systèmes d'information et de leurs échanges.
- Maitriser la norme BPMN (Business Process Model & Notation) qui permet aux entreprises de décrire de façon structurée et efficace leurs processus.
- Apprendre une méthodologie de mise en œuvre d'une démarche processus dans une entreprise. *(Étant donné la complexité de l'environnement des entreprises, cette mise en œuvre se fait par étapes.)*
- Mettre en perspective de la vision BPM avec d'autres méthodologies.

À qui s'adresse cette formation ?

Public :

Ce cours cible toute personne en charge de la sécurité souhaitant structurer efficacement les processus à mettre en place au sein de son entreprise.

Prérequis :

Sont concernées par cette formation, les personnes impliquées par la Cybersécurité, et qui souhaitent apporter de la rigueur et de l'efficience à leurs processus dans ce domaine, que ceux-ci soient opérationnels ou de gouvernance.

Contenu du cours Cybersécurité BPM

Vision processus

Concepts et définitions.
Types de processus de cybersécurité concernés : opérationnels (ex : campagnes de tests d'intrusion) et de gouvernance (ex : revue d'un outil de gestion des risques)
Les 2 principaux modèles de BPMN 2.0.

Modélisation de processus

Aborder la modélisation d'un processus.

Présentation de Signavio ™ Quick Model.

Présentation de Bizagi ™ Modeler.

Composantes de base de BPMN 2.0.

Atelier

Modélisation simple de processus en cybersécurité, opérationnels et de gouvernance.
L'atelier peut porter sur les processus prévus dans la formation, ou sur des processus à la demande des stagiaires.

Mise en œuvre par étapes

Audit de cybersécurité.

Modélisation simple de processus de sécurité.

Modélisation avancée de processus de sécurité.

Exécution de processus.

Suivi de processus avec un BAM (Business Activity Monitoring).

Atelier

Réflexion sur la mise en œuvre dans un cas concret. Liste de livrables à l'issue de cette réflexion.
L'atelier peut porter sur le processus prévu dans la formation, ou sur un processus à la demande des stagiaires.

Mise en perspective de la vision BPM avec d'autres méthodologies

BPM et Lean Six Sigma.

BPM et ITIL.

BPM et normes ISO.

BPM et ISM (Information Security Management).

Atelier

Etude de l'existant dans l'entreprise des stagiaires.

Travaux Pratiques

Cette formation se base sur la connaissance d'un cas réél pour structurer son apport pratique : **(Dans le cadre d'une demande en INTRA Entreprise, les ateliers sont orientés en fonction de l'existant dans l'entreprise.)**

Exemple :
Une grande entreprise française dans le domaine de l'énergie s'est retrouvée confrontée à des problématiques de sécurité. En sachant que ses activités lui imposent d'importantes réglementations dans ce domaine.

La méthode employée a consisté à réunir les responsables métier pour qu'ils mènent collectivement des analyses contextuelles de risque, sachant qu'un risque est constitué dès lors qu'un agent menaçant – humain ou automatisé – parvient à exploiter une vulnérabilité sur un actif métier, en contournant les mesures de protection existantes.

Les métiers ont été tenus de définir leurs besoins en sécurité (en confidentialité, en disponibilité, en intégrité ou en traçabilité) sur les actifs qu'ils captent, gèrent, diffusent et stockent, afin de révéler les actifs prioritaires pour l'entreprise.

Pour réussir à adopter un langage commun, les salariés ont dû faire appel à la modélisation de leurs processus et de leurs flux de données. L'idée était de ne pas partir d'une feuille blanche mais de ce que les métiers connaissent déjà : les processus auxquels ils font appel au quotidien.

En partant de leurs processus, les parties prenantes de l'entreprise ont dû imaginer des scénarios de contournement, en se mettant dans la peau de différents profils d'attaquant (hacker malveillant, fournisseur négligent, ancien collaborateur mécontent, …) et ainsi identifier et mesurer les risques.