SAS IFOR
139 Rue du Faubourg Saint Honoré
75008 PARIS
T. 01 42 56 49 67
F. 01 42 25 52 61
www.ifec.fr

Cartographie des risques de cyber-attaques

PUBLIC

Collaborateurs ; Commissaires aux comptes ; Experts-comptables

DUREE

1 jour(s) - 7 h

Nb minimum de participants : 8

PRE REQUIS

AUCUN

OBJECTIFS PEDAGOGIQUES

- Comprendre les cyber-attaques : leur type, leur mécanisme et leurs conséquences.
- Identifier les risques pour son entreprise.
- Évaluer les risques et en limiter les impacts

CONTENU PEDAGOGIQUE

Cyber-attaques, les enjeux actuels dépassent le risque opérationnel
L'augmentation exponentielle des cyber-attaques et de leurs impacts économiques et sociétaux.
L'origine du cyber-risque : la digitalisation des activités et la complexification technologique.
Les nouveaux territoires virtuels.
Connaître la typologie de cyber-attaques et leurs mécanismes
Enjeux et propriétés du cyberespace.
Définition et anatomie des cyber-attaques.
La classification des cyber-attaques et leurs impacts : cybercriminalité, atteinte à l'image, espionnage, sabotage.
Quelles sont les menaces et vecteurs de menaces ?
Quelles sont les motivations, les profils des hackers ?
Quels sont les équipements qui sont visés, dans quel but et comment ?
Les principales cyber-attaques qui affectent aujourd'hui les entreprises :
Le phishing (hameçonnage et harponnage) ;
Les dénis de services distribués (DDos) ;
L'installation de programmes espions ;
Le vol d'informations stratégiques ;
Le ransomware (rançongiciel) ;

IFOR SAS inscrite au Registre du Commerce et des Sociétés de Paris sous le numéro 798 126 645 SIRET : 79812664500018 - N° TVA Intracommunautaire : FR 347981264500018 N° Déclaration d'Activité :11 75 23457 75

L'attaque des sites internet ;
etc. sous-puce-pgm
Le vocabulaire à connaître : cheval de Troie, virus/vers, spyware et keylogger, ransomware, vulnérabilité et exploits, etc.
Quelques bonnes pratiques de sécurité et d'hygiène numérique
Évaluer et gérer les cyber-risques de son entreprise
Méthode de gestion des risques cybernétiques.
Normes 2700x au service du management de la sécurité
Audit, pentest, bug bounty
Dispositif d'amélioration continue
Réaliser l'inventaire des actifs primordiaux.
Identifier les menaces et vecteurs de menaces.
Connaître ses faiblesses et vulnérabilités.
Évaluer la vraisemblance et l'impact potentiel des risques identifiés.
S'organiser pour limiter les impacts
Rédiger une charte et/ou une politique SSI.
Comment détecter une cyber-attaque pour mieux s'en défendre.
Tableaux de bord, indicateurs et plan d'action.
Continuité et reprise d'activité (PCA/PRA)
Gestion de crise.
Dispositif d'amélioration continue.

MOYENS & METHODES PEDAGOGIQUE

Cas pratiques et d'exemples concrets, alliés à des connaissances techniques
Interactivité entre participants et intervenant
Support est remis en début de formation à chaque participant

EVALUATION DE LA FORMATION / SANCTION DE LA FORMATION

. Délivrance d'une attestation individuelle de formation.

DEROULEMENT

Horaires : 9 h - 17 h3 0
Déjeuner : le déjeuner est libre, le créneau de celui-ci est défini par l'animateur
Nombre minimum de participants : 8
Nombre maximum de participants : 18

FORMATEUR

Régis LE GUENNEC

Consultant Francis Lefebvre Formation

TARIFS HT:

Adhérent IFEC : 709 €
Adhérent IFEC + CJEC : 600 €
Adhérent IFEC + ANECS : 600 €
Adhérent IFEC + Stagiaire : 600 €
Adhérent IFEC +Inscrits à l'ordre < 5ans : 600 €
Non Adhérent IFEC : 927 €

IFOR SAS inscrite au Registre du Commerce et des Sociétés de Paris sous le numéro 798 126 645 SIRET : 79812664500018 - N° TVA Intracommunautaire : FR 347981264500018 N° Déclaration d'Activité :11 75 23457 75