CYBERSECURITE (A DESTINATION DES COLLABORATEURS IT)

Pôle d'activité

PREVENTION ET SECURITE

Formule

Présentiel

Prix/participant

300,00 €
Gratuité possible : consultez les conditions sur notre site.

Nombre max. de participants/session

12

Durée de la formation

3 jours (8h30-16h30)

Personne de contact

Lamia MALLOULI Responsable du service Secrétariat

lmallouli@erap-gsob.brussels

Détail de la formation

Le domaine de la cyber sécurité évolue très rapidement et de nouveaux défis ne cessent d'émerger. Les cas de piratage informatique, de violation de données, de fraude électronique, d'interruption de services administratifs ou de perturbation de leurs infrastructures arrivent encore trop régulièrement. Pour faire face à cette problématique et afin de répondre aux besoins des administrations locales et régionales, l'ERAP a élaboré un programme visant à apporter davantage de clarté ainsi qu'à donner des outils afin de lutter contre la cybercriminalité. Ce programme est décliné en deux modules de formations, adapté au niveau de responsabilité de chacun.

Le présent module offre une base de référence cohérente, qui permettra aux collaborateurs des services IT (IS Engineers, Analystes Développeurs, …) issus des administrations locales et (para) régionales, d'implémenter les mesures et les systèmes de sécurité informatiques.

Ces programmes s'inscrivent dans le cadre du Plan Global de Sécurité et de Prévention (PGSP) et de Brusafe.

Vous êtes IT manager et/ou vous gérez une équipe ? Un second module de 2 journées vous est proposé afin d'élaborer et d'implémenter une stratégie cyber sécurité au sein de votre organisation.

Objectifs

- Permettre aux participants d'avoir des notions communes avec les IT managers afin de faciliter la communication renforcer les équipes.
- Permettre aux participants de détecter des failles dans un serveur et à apporter des sécurités efficaces et reconnues dans le milieu de la cyber-sécurité.
- Aider les participants à comprendre les attaques venant d'internet et de trouver une solution avec eux afin de construire une sécurité appropriée à leurs infrastructures.
- Permettre aux participants de pouvoir continuer leur apprentissage après la formation et les rendre capables de s'entrainer seuls.
- Proposer aux participants des pistes d'amélioration de leur(s) infrastructure(s) pour assurer une protection régulière de leur administration/organisation au niveau de la cyber sécurité.
- Permettre aux participants d'auditer la sécurité des applications web de leur administration/organisation et proposer des solutions aux personnes en charge du développement de ces plateformes.
- Travailler avec les participants pour les aider à comprendre « la solution » afin qu'ils puissent l'intégrer ou intégrer une solution similaire à leur infrastructure.

Public cible

La formation est destiné aux collaborateurs IT des pouvoirs locaux ou régionaux bruxellois et des organismes d'intérêt public bruxellois ci-dessous.

Institutions visées (non-exhaustif) :
- Communes
- CPAS
- Centre d'Informatique pour la Région Bruxelloise
- Bruxelles Propreté
- Bruxelles Environnement
- Zones de Police Bruxelloises
- Service Public Régional de Bruxelles
- Bruxelles Prévention Sécurité
- Ecole Régionale des Métiers de la Sécurité, de la Prévention et du Secours
- Société du Logement de la Région Bruxelloise
- …

Méthodes pédagogiques

Résolument axée sur la pratique, illustrée d'exemples adéquats et animée par des inter venants spécialistes de la matière traitée, cette formation se veut très interactive et basée sur des cas concrets. Pour ce faire, le formateur / la formatrice alterne les styles pédagogiques et les thèmes sont abordés via des méthodologies pratiques et actives permettant de mettre les bénéficiaires au centre de la formation et d'être régulièrement en interaction à l'aide d'exercices en groupe.

Contenu

Gestion de la cyber-sécurité

- Identifier la Hack-Value
- Mitiger le risque
- Gestion de l'hygiène de la cyber-sécurité
- Gestion des incidents

Présentation des outils de piratage

- Méthodologie d'un piratage
- Présentation et exercices sur Kali Linux
- Présentation et exercices sur NMAP
- Présentation et exercices sur Metasploit

Sécurité des postes de travail

- Metasploit et NMAP : attaque sur un poste de travail
- Sécuriser un poste de travail
    - Anti-Virus/Anti-Malware
    - Cryptage des disques
    - Gestion des programmes
- Gouvernance
    - Gestion des utilisateurs
    - Séparation des comptes utilisateurs et administrateurs
    - Utilisation d'authentification à multiples facteurs

Sécurité des serveurs

- Metasploit et NMAP : attaque sur un serveur
- Sécuriser un serveur
    - Sécuriser un serveur Web (Apache et NGINX)
    - Gestion de bases de données (SQL et No-SQL)
    - Gestion des droits
- Gouvernance
    - Gestion des accès de droits
    - VPN

Sécurité des réseaux (LAN)

- Réseau local (LAN)
    - La reconnaissance via l'utilisation de NMAP
    - L'attaque d'un réseau via NMAP
    - Sécuriser le réseau au moyen de VLAN
    - Sécuriser les accès au réseau (wifi + accès physique)

    - Exercice sur la mise en place d'un IDS/IPS (détection d'intrusion)
- Réseau local (WAN)
    - L'attaque sur un pare-feu
    - Comment configurer un pare-feu
    - Gestion de la charge

Théorie de la cyber-sécurité

- L'encryptions
- Les outils dans le Cloud
    - Azure Active Directory
    - Scanners en ligne
    - Ressources en ligne
- S'entrainer en ligne
    - Présentation de plateformes permettant de s'entrainer en ligne à la sécurité informatique
    - Présentation de sites internet permettant d'améliorer ses connaissances

Sécurité avancée

- L'hyperconnexion de la sécurité de l'information
- Gestion des accès et des droits (IAM)
- Fonctionnement d'un SIEM (Security Information and Event Manager)
- Fonctionnement d'un SOC (Security Opération Center)

La sécurité d'une application web

- Attaque d'une application web via Kali Linux
- Présentation d'OWASP
- Recherche de sécurité pour application web

Exercice : Implémentation d'une solution SIEM

- Présentation de la solution Open-Source ELK
- Mise en pratique : exercice