SQLI INSTITUT

400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

ÉTAT DE LCODE2UTF('8217',0)ART DE LA SÉCURITÉ DES SYSTÈMES DCODE2UTF('8217',0)INFORMATION

CODE STAGE : S-SEC

OBJECTIFS

Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
Connaître les principes et les normes de chaque domaine de la SSI
Disposer d'informations sur les tendances actuelles, que ce soit dans les menaces ou dans les solutions à notre disposition

DURÉE

3 jours

PUBLIC

Directeurs des systèmes d'information ou responsable informatique, RSSI, chefs de projet sécurité, architectes informatiques

PRÉ-REQUIS

Pas de pré-requis

PROGRAMME

EVOLUTIONS DES MENACES ET LES RISQUES
Statistiques sur la sécurité : tendances dans l'évolution des menaces

MODÈLE D'APPROCHE ET MATURITÉ EFFECTIVE DE L'ORGANISME
Identification des acteurs : organisation et responsabilités
Exigences SSI : obligations légales métiers, responsabilités civiles, responsabilités pénales, règlements, délégations

L'IDENTIFICATION DES BESOINS DICP
Classification SSI : informations, données et documents, processus, ressources, les pièges
Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

L'ÉTAT DE L'ART DES MÉTHODOLOGIES ET DES NORMES

Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients

Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients

Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients

MODÉLISATION DES NIVEAUX DE MATURITÉ DES TECHNOLOGIES SSI

Les choix structurants et non structurants et positionnements

La sécurité des accès : filtrage réseau, identification, authentification, gestion des identités vs. SSO, habilitation, filtrage applicatif, détection/protection d'intrusion, journalisation

La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP

Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation

NOMADISME

Sécurité des postes nomades : problèmes de sécurité liés au nomadisme, protection d'un poste vs. Solutions spécifiques, mise en quarantaine, accès distants, VPN Concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

LES ARCHITECTURES DE CLOISONNEMENT

La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

LA SÉCURITÉ DES END POINT

Le durcissement : postes de travail, ordi phones, serveurs

L'adjonction d'outils : postes de travail, ordi phones, serveurs

La sécurité des applications : les standards et les bonnes pratiques