Formation Réaction aux incidents de sécurité selon ISO 27035

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Les entreprises et les administrations ont mis en oeuvre de nombreuses mesures de prévention en matière cybersécurité mais les mécanismes de détection et surtout de réaction sont souvent moins avancés. Les vulnérabilités exploitables sont nombreuses et nul n'est à l'abri d'un incident majeur impactant la sécurité des systèmes d'information de son entité. Cette formation de 2 jours vous permettra d'acquérir les connaissances et mettre en place les outils indispensables pour élaborer un processus solide de détection et de réaction aux incidents de sécurité. La formation est destinée à toute personne amenée à mettre en place ou à intervenir dans la gestion des incidents de sécurité : DSI, RSSI, responsable Security Operation Center, responsables production, consultants.

Référence	RIC12
Durée	2 jours (14h)
Tarif	à partir de 1 300 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| catégoriser des événements et des incidents, cartographie de cas réels récents, normes et documentations disponibles.
| élaborer un processus de gestion des incidents de sécurité : processus de veille, détection, qualification, réaction, outils disponibles, reporting, interactions avec la politique de sécurité, rôle du SOC, communications internes et externes, composition et fonctionnement de la cellule de réaction aux incidents, tableau de bord des incidents, liens avec les processus ITIL.
| Connaître l'environnement extérieur : les services de gendarmerie et de police, l'agence nationale de sécurité des systèmes d'information, les médias, les CERT (computer and emergency response team).
| Connaître les aspects légaux et réglementaires : fraudes, dépôt de plainte, forensics.
| gérer une crise : incidents et crises, capacité à gérer une crise, comment se préparer, évaluer une situation, prendre des décisions, maîtriser la communication.

Public

| DSI
| RSSI
| Responsable Security Operation Center
| Responsables production
| Consultants
| Etc...

Prérequis

| Une première expérience dans le domaine de la sécurité de l'information est fortement recommandée

Programme de la formation

Catégorisation des événements et des incidents de sécurité :
| Cartographie de cas réels
| Revue des normes et documentations disponibles

Elaboration d'un processus de gestion des incidents de sécurité :
| Veille, détection, qualification et réaction, outils disponibles, reporting
| Interactions avec la politique de sécurité
| Rôle du SOC

| Communications interne et externe
| Composition et fonctionnement de la cellule de réaction aux incidents
| Tableau de bord des incidents
| Liens avec les processus ITIL

Environnement extérieur :
| Les services de gendarmerie et de police
| L'agence nationale de sécurité des systèmes d'information
| Les CERT (computer and emergency response team)

Etude et résolution de cas concrets :
| DDoS
| Attaque ciblée

Aspects légaux et réglementaires :
| Cadre légal français
| Fraudes informatiques
| Dépôt de plainte
| Investigations, « forensics »

Gestion des crises :
| Incidents et crises
| Capacité à gérer une crise :

Se préparer
Evaluer une situation
Prendre des décisions
Maîtriser la communication
Etude et résolution de cas concrets :
| Défiguration de site WEB
| Divulgation d'un document stratégique

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.