Séminaire de 2 jour(s)
Réf : BYR

Participants

RSSI, Fonction SSI, direction générale, DSI, juristes.

Pré-requis

Aucune connaissance particulière.

Prix 2020 : 1990€ HT

Dates des sessions

CLASSE A DISTANCE
03 déc. 2020
PARIS
03 déc. 2020

Modalités d'évaluation

Les apports théoriques et les panoramas des techniques et outils ne nécessitent pas d'avoir recours à une évaluation des acquis.

Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.

• A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation

Cybercriminalité et Cyberguerre, enjeux et défis

La cybercriminalité est une menace grandissante sur la société. Les cybercriminels agissent de n'importe où pour s'attaquer aux infrastructures des entreprises. La question abordée dans ce cours ne sera pas de savoir si votre organisme sera attaqué mais de se préparer, détecter, anticiper et gérer les cybercrises.

OBJECTIFS PEDAGOGIQUES

Connaître les dangers et identifier les sources de menaces
Comprendre les risques et les enjeux de sécurité
Détecter les intrusions et réagir face aux malveillances
Savoir organiser une riposte efficace, utile et graduée
Planifier son plan de crise face à la cyberguerre

Méthodes pédagogiques

Présentation magistrale avec faits et incidents de sécurité réels et récents et jurisprudence en France et en Europe.

1) Cybercriminalité dans l'actualité

- Données sensibles : cyber vols, espionnage.
- Nouvelle guerre froide Est/Ouest, USA/Chine.
- Dénis de services d'envergure mondiale.
- Hackers organisés, rôle des agences de renseignements.
- Actualité : malwares, bots/botnets, ransomwares.
- APT (Advanced Persistant treat), infractions aux CB, skimming.

2) Détecter les intrusions

- Gestion des traces, preuves, enregistrements.
- Détecter une activité anormale, signaler un incident.
- Analyse et corrélation d'évènements de sécurité (SIEM).
- Pertinence du SOC (Security Operation Center).
- Automatiser la gestion des incidents.
- Tests d'intrusion, mesure d'anticipation incontournable.
- Recourir à une société spécialisée de détection des incidents.

3) Organiser la riposte

- Recherche et collecte de preuves.
- Déclarer un incident, préparer sa communication de crise.
- Rôle des CERTs.
- Cellule de crise : organiser, gestion de la crise.
- Gestion des vulnérabilités et patch management.

4) Ordre étatique face à la cybercriminalité

- Cyber délits (France, Europe) : quel dispositif répressif ?
- Rôle de l'ANSSI (France) et de l'ENISA (Europe).
- Gestion de la preuve : recevabilité, collecte sur Internet.
- Directive européenne Network and Information Security (2018).
- Règlement Européen « cyber security Act » (2019).
- Loi de Programmation Militaire (2016).
- Rôle des états et de l'Europe : lois, directives et règlements.

5) Les bonnes pratiques types OIV / OSE

- Gouvernance de la cybersécurité : rôles, responsabilités, implication des métiers dans la gestion des risques.
- Défense en profondeur : politique de contrôle d'accès, gestion des comptes à privilège.
- Gestion des incidents de cybersécurité : politique de détection, réaction.

6) Le Maintien en Condition de Sécurité

- Politique de gestion des vulnérabilités, traitement (correctif).
- Périmètres sensibles : gestion des mises à jour.
- Déclaration des attaques subies.
- Prestataires certifiés obligatoires (PDIS, PRIS).
- Audit de sécurité par l'ANSSI, recours aux auditeurs certifiés (PASSI, LPM).

ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.