Formation Cybersécurité : élaborez votre vision stratégique

Un panorama complet pour assurer la cyber-résilience de votre entreprise

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

Référence	MOTC
Durée	3 jours (21h)
Tarif	2 960 €HT
Repas	repas inclus

Objectifs

| Identifier les risques liés à la cybercriminalité et les enjeux de la cybersécurité
| Maitriser les aspects techniques, juridiques et organisationnels de la cybersécurité
| Assurer la continuité d'activité et la sécurité des données dans le cloud
| Elaborer une riposte adéquate et proportionnée pour réduire les risques cyber

Public

| RSSI
| DSI
| Chefs de projet cybersécurité
| Responsables cellule de crise
| Ingénieurs d'études
| Concepteurs
| Auditeurs IT
| Consultants

Prérequis

| Aucun

Programme de la formation

Comprendre la cybercriminalité et les enjeux
| L'impact économique de la cybercriminalité et le modèle économique du « Crime as a Service »
| Analyse de la menace cyber (CTI) et techniques d'attaque (Framework MITTRE ATT&CK)
| Ransomware (rançongiciel) : la menace cyber numéro 1 dans le monde
| Panorama des cyberattaques contre les entreprises et les infrastructures critiques
| Le rôle des crypto-monnaies (Bitcoin, Dash, Monero, Zcash,...) dans les opérations cybercriminelles

Maîtriser les principes fondamentaux de cybersécurité
| Les 7 principes fondamentaux : défense en profondeur, moindre privilège, besoin d'en connaître,...
| Assurer la cybersécurité via une approche gestion des risques ou par la conformité
| Les vulnérabilités logicielles : identification (CVE), criticité (CVSS) et cycle de vie
| Panorama des normes ISO 2700x et zoom sur l'ISO 27001 & 27002
| Les sources d'informations incontournables (ANSSI, ENISA, NIST, CIS, CSA, OWASP, CESIN, ...)

Identifier le cadre juridique et règlementaire
| Les principales lois Cyber en France et la hiérarchie des normes juridiques
| La directive européenne NIS2 (Network and Information Security)
| Le règlement européen pour la protection des données personnelles (RGPD)
| Le règlement européen pour les certifications de sécurité (Cyber Security Act)
| Le règlement européen pour la sécurité de l'IoT et de la supply chain (Cyber

PROCHAINES SESSIONS

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

Resilence Act)

Organiser la cybersécurité
| La politique de sécurité (PSSI) : structure, application et contrôle
| Le rôle et les responsabilités des RSSI et DPO, leurs relations avec la DSI, la DG et la CNIL
| Les métiers de la cybersécurité : auditeur, pentester, consultant, risk manager, SOC analyst, ...
| Sensibilisation à la sécurité : pour qui ? pourquoi ? comment ?
| La charte de sécurité : existence légale, contenu et sanctions

Financer la cybersécurité
| Quel budget faut-il allouer à la cybersécurité ? les recommandations de l'ANSSI
| Comment définir le Return On Security Investment (ROSI) ?
| Quel est l'impact financier d'un incident de sécurité ? exemples et chiffres disponibles
| Financer le risque Cyber par une cyber-assurance : périmètre, garanties et limites

Identifier les principales solutions techniques
| Sécurité réseau : Firewall NG, UTM, WAF, SASE, Zero Trust, NDR, ...
| Sécurité des « Endpoints » : antimalware (EPP) et solutions de nouvelle génération (EDR / XDR)
| Chiffrement des systèmes : Bitlocker, Luks, FileVault, Veracrypt,...
| Protection des clés et des secrets : gestionnaires de mots de passe, TPM, HSM
| Sécurité de l'authentification : MFA, FIDO2, biométrie. Solutions « passwordless »
| Sécurité des développements logiciels : les activités de sécurité applicative d'un Secure SDLC

Sécuriser les données dans le Cloud computing
| Les principaux risques dans le Cloud et les mesures de sécurité associées
| Les solutions de sécurité spécifiques au Cloud : CASB, CWPP, CSPM et SSPM
| Le chiffrement dans le Cloud (BYOK, BYOE) et exigences dans la certification de sécurité EUCS
| Les 5 façons d'évaluer la sécurité d'un fournisseur Cloud
| L'approche française du Cloud souverain vs Cloud de confiance
| L'impact des lois américaines (Patriot Act., FISA et Cloud Act) sur la sécurité des données

Assurer la continuité d'activité
| Principes BC/DR : résilience vs continuité d'activité vs reprise d'activité
| Les fondamentaux de la gestion de la continuité d'activité (BCM)
| Réaliser un bilan d'impact sur l'activité (BIA) : différence avec l'analyse de risques
| Les métriques et exigences de la continuité : SLA, SLO, MTD, RTO, RPO, WRT
| Gestion des sauvegardes de données

Contrôler et superviser la cybersécurité
| Audits de sécurité, tests d'intrusion et programmes de Bug bounty
| Tableaux de bord de sécurité : indicateurs, KPI, KPSI, KRI et référentiels (SP 800-55, ETSI GS ISI,...)
| Agences de notation du risque Cyber (BitSight, SecurityScorecard, Cyrating, ...)
| Le rôle et les activités d'un CERT / CSIRT
| Le rôle d'un SOC (Security Operation Center) et les outils SIEM / SOAR pour superviser la sécurité

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.