Dates : sur devis

Formation intra-entreprise
Certification : NON

État de l'art de la sécurité des systèmes d'information

Mise à jour févr. 2025

Durée 3 jours (21 heures)

« Délai d'accès maximum 1 mois »

OBJECTIFS PROFESSIONNELS

- Comprendre les menaces sur les équipements de l'infrastructure
- Mettre en place une politique interne (technologique et humaine) de sécurité des informations
- Choisir les dispositifs et emplacements de sécurité
- Concevoir le Plan de Sécurité

PARTICIPANTS

-

PRE-REQUIS

- DSI, RSSI, RSI, Technicien sécurité

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Remise d'un support de cours.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Prévention / Sécurité

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Programme de formation

1. Domaines et contours de la sécurité (00h15)

Domaines et contours de la sécurité (02h15)

- Les systèmes de gouvernance
- Les systèmes de gouvernance
- Présentation des risques involontaires
- Présentation des risques involontaires
- Cybercriminalité
- Cybercriminalité
- Le cycle de la gouvernance
- Le cycle de la gouvernance
- Les organes de contrôle
- Les organes de contrôle
- Le contrôle Interne
- Le contrôle Interne
- Les audits externes
- Les audits externes
- Les acteurs de la sécurité
- Les acteurs de la sécurité
- Environnements juridiques
- Environnement juridiques
- Droits et obligations des entreprises en termes de sécurité
- Droits et obligations des entreprises en termes de sécurité
- La loi Sécurité Financière SOX (Sarbane Oxley) , La CNIL
- La loi Sécurité Financière SOX (Sarbane Oxley) , La CNIL

2. Analyse des risques (00h15)

Analyse des risques (03h00)

- Connaître son SI
- Connaître son SI
- PC final
- PC final
- Serveur
- Serveur
- Utilisation d'une ferme de serveurs
- Utilisation d'une ferme de serveurs
- Quelles sont les données externalisées (cloud) ?
- Quelles sont les données externalisées (cloud) ?
- Matériel réseau
- Matériel réseau
- Méthodes d'accès aux réseaux
- Méthodes d'accès aux réseaux
- Méthodes d'identification
- Méthodes d'identification
- Gestion des autorisation
- Gestion des autorisations
- Risques de piratage
- Risques de piratage
- Risques de perte d'information
- Risques de perte d'information
- Risques de vols d'information
- Risques de vols d'information
- Risques naturels
- Risques naturels
- Les pannes matérielles
- Les pannes matérielles
- Les risques d'ingénierie sociale
- Les risques d'ingénierie sociale

Mise en oeuvre d'une politique de sécurité (00h15)

3. Mise en oeuvre d'une politique de sécurité (03h30)

- La sécurité physique
- La sécurité physique
- Accès aux installations
- Accès aux installations
- Sécurité des installations (incendies, inondations, vols...)
- Sécurité des installations (incendies, inondations, vols...)
- Prévision d'un plan de continuité et de reprise
- Prévision d'un plan de continuité et de reprise
- Contrôler les accès
- Contrôler les accès
- La sécurité des services
- La sécurité des services
- Sécuriser les applications
- Sécuriser les applications
- Cryptage
- Cryptage
- Technologies VPN
- Technologies VPN
- VPN SSL
- VPN SSL
- HTTPS
- HTTPS
- Sécurité des protocoles Peer-to-peer
- Sécurité des protocoles Peer-to-peer
- Blocage des applications
- Blocage des applications
- Sécurité des terminaux mobiles
- Sécurité des terminaux mobiles
- Utilisation d'une DMZ
- Utilisation d'une DMZ
- Comment intégrer la disponibilité et la mobilité des collaborateurs
- Comment intégrer la disponibilité et la mobilité des collaborateurs
- Généralités sur les outils disponibles

- Généralités sur les outils disponibles

4. Les aspects organisationnels de la sécurité (00h15)

Les aspects organisationnels de la sécurité (02h00)

- Définition des risques
- Définition des risques
- Confidentialité
- Confidentialité
- Intégrité
- Intégrité
- Supervision
- Supervision
- La veille technologique
- La veille technologique
- Publication des failles
- Publication des failles
- Principe du modèle de maturité
- Principe du modèle de maturité
- Sécurité du système d'exploitation
- Sécurité du système d'exploitation
- Gestion des privilèges
- Gestion des privilèges
- Documentation
- Documentation

Management de la sécurité (00h15)

5. Management de la sécurité (03h00)

- Les méthodes Méhari EBIOS ISO 27001 Cobit
- Les méthodes Méhari EBIOS ISO 27001 Cobit
- Les limites de ces méthodes
- Les limites de ces méthodes
- Les audits de sécurité
- Les audits de sécurité
- Mener un audit dans une entreprise multisites
- Mener un audit dans une entreprise multisites
- Trop de sécurité tue la sécurité, comment éviter les faux-positifs
- Trop de sécurité tue la sécurité, comment éviter les faux-positifs
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- La roue de la sécurité
- La roue de la sécurité
- Mise en oeuvre technique de la sécurité
- Mise en oeuvre technique de la sécurité
- Stress du système
- Stress du système
- Amélioration de la sécurité
- Amélioration de la sécurité
- Savoir protéger les investissements au meilleur coût pour les meilleures raison
- Savoir protéger les investissements au meilleur coût pour les meilleures raisons
- Communications sur la politique de sécurité
- Communications sur la politique de sécurité
- Comment réagir à une attaque (en interne, en externe)
- Comment réagir à une attaque (en interne, en externe)
- Les limites du plan de sécurité et les dispositions juridiques
- Les limites du plan de sécurité et les dispositions juridiques
- Définition et rôle du RSSI
- Définition et rôle du RSSI

6. Méthodologie et technologie (00h15)

Méthodologie et technologie (02h00)

- La vision de la sécurité selon les interlocuteurs
- La vision de la sécurité selon les interlocuteurs
- Les objectifs
- Les objectifs
- Les moyens techniques et financiers mis en oeuvre
- Les moyens techniques et financiers mis en oeuvre
- La stratégie
- La stratégie
- L'adaptation et la gestion du changement
- L'adaptation et la gestion du changement
- Elaboration du plan de sécurité
- Elaboration du plan de sécurité
- L'audit de conformité
- L'audit de conformité
- Les indicateurs
- Les indicateurs
- Les tableaux de bords à établir
- Les tableaux de bords à établir
- Les méthodologies d'audit
- Les méthodologies d'audit

Les outils (00h15)

7. Les outils (03h00)

- Fonction d'un firewall
- Fonction d'un firewall
- Documentation des accès autorisés sur le réseau
- Documentation des accès autorisés sur le réseau
- Création d'une charte d'utilisation du réseau pour les collaborateurs
- Création d'une charte d'utilisation du réseau pour les collaborateurs
- Fonction d'un système de détection d'intrusion
- Fonction d'un système de détection d'intrusion
- Les logiciels clients de sécurité (firewall, antivirus, antispyware...)
- Les logiciels clients de sécurité (firewall, antivirus, antispyware...)
- Superviser la sécurité
- Superviser la sécurité
- Faire évoluer la sécurité

- Faire évoluer la sécurité
- Contraction d'assurances : quelles sont les garanties ? qu'est ce qui peut et doit être assuré ? l'importance de la disponibilité du système
- Contraction d'assurances : quelles sont les garanties ? qu'est ce qui peut et doit être assuré ? l'importance de la disponibilité du système
- Validation technique de l'architecture
- Validation technique de l'architecture
- Formation des personnels du SI
- Formation des personnels du SI
- Formation des utilisateurs du SI
- Formation des utilisateurs du SI
- Avenir de la sécurité informatique
- Avenir de la sécurité informatique
- Les 6 idées les plus stupides selon Marcus J. Ranum
- Les 6 idées les plus stupides selon Marcus J. Ranum
- La vision géostratégique de la sécurité
- La vision géostratégique de la sécurité
- Les phénomènes de monopole
- Les phénomènes de monopole

8. Rédaction de chartes d'utilisation et / ou de configuration (00h15)

Rédaction de chartes d'utilisation et / ou de configuration (01h30)

- Le secret professionnel
- Le secret professionnel
- Le respect de la législation
- Le respect de la législation
- Les règles de confidentialité
- Les règles de confidentialité
- L'usage des services Internet
- L'usage des services Internet
- Définir sa charte d'utilisation
- Définir sa charte d'utilisation
- Responsabilités du comité de coordination du SI
- Responsabilités du comité de coordination du SI
- Responsabilités du conseil d'administration et des représentants
- Responsabilités du conseil d'administration et des représentants