

Durée : 1 jour (8h)

Tarif : 890 € HT

Horaires :

De 08 h 30 à 12 h 30

De 14 h 00 à 18 h 00

Public :

Expert en sécurité et système d'information.

Responsable technique.

Expert domaine infrastructure.

Responsable infrastructure.



WASQUEHAL

Nous consulter pour connaître les disponibilités.



10 personnes

Intervenant :

A définir

Pédagogie :

Les cours regroupent des enseignements théoriques et des ateliers pratiques.

À l'issue de chaque cours, les participants sont invités à passer un examen des connaissances.

Évaluation :

Chaque exercice proposé par module est contrôlé et doit être réussi, si cela n'est pas le cas, l'exercice est repris jusqu'à l'acquisition complète.

Renseignements :

Tél : 03 28 32 11 11

contact@partnersystemes.fr

Lieu de la formation :

Partner Systèmes

10 Av du Gd Cottignies

59290 Wasquehal

PARTNER SYSTEMES

10 Av du Gd Cottignies - 59290 Wasquehal

contact@partnersystemes.fr

https://www.partnersystemes.fr

Code APE 4666Z - N° de Siret 753 916 485 000 18

CYBERSÉCURITÉ DE KASPERSKY LAB

PROGRAMME

Formation complète allant des techniques de cyber diagnostic à l'analyse des programmes malveillants et des mesures de sécurité.

OBJECTIFS

Comprendre les risques associés à l'ère du numérique.

Adopter les meilleures pratiques de gestions et d'informations de la sécurité .

Maîtriser les fondamentaux des standards du marché comme ISO 27001.

Mettre en place un système de management pour la sécurité.

Identifier les menaces et comprendre les déploiements techniques à mettre en oeuvre.

PRÉ-REQUIS

Il est recommandé d'avoir des compétences sur l'organisation d'un système informatique pour suivre la formation cybersécurité.

CONTENU

■ L'environnement de la cybersécurité et le cadre juridique

- Retour sur la réglementation RGPD (Règlement Général sur la protection des données).
- Identifier les risques juridiques en cas d'infraction à votre système informatique.
- L'environnement de la cyber criminalité, focus sur les organisations criminelles et associations de malfaiteurs.
- Le cadre spécifique du vol d'informations.
- Mise en place de charte informatique auprès des salariés.

■ Retour sur la notion de danger en cyber criminalité

- Appréhender les dernières méthodes criminelles utilisées en cyber criminalité et déterminer une cartographie des risques majeurs.
- Le piratage des données ou des serveurs.
- Le principe du hacking.
- L'hameçonnage, phishing ou le filoutage.
- La méthode des demandes de rançon.

■ Les mesures de prévention pour les entreprises

- Quels sont les principes et les incontournables d'une bonne PSSI (politique de sécurité des systèmes d'information) ?
- Les principes de sécurité liés aux risques internes.
- Les principes de sécurité liés aux risques externes.
- Développer l'expertise de son SSI (système de sécurité incendie) mais aussi la connaissance générale du personnel (en particulier les cadres et les dirigeants).
- Le défi du SSI : comment sécuriser les échanges sans alourdir les procédures ni provoquer des comportements d'évitement.
- Se prémunir des actes malveillants pouvant intervenir via une messagerie.
- Comment sécuriser ses déplacements professionnels ?
- Sensibilisation liée aux risques de Faux Ordres de Virement (FOVI).

■ Savoir gérer une cyber attaque

- Identifier des outils simples et efficaces à mettre en œuvre pour vérifier que le système d'information n'est pas déjà compromis.
- Recherches et analyses des traces sur supports numériques ; techniques d'OSINT (Open Source INTelligence).
- Analyse de la mémoire vive.
- Comment récolter les traces lors d'une attaque afin de permettre un dépôt de plainte ultérieur efficace tout en rétablissant au plus vite le système pour que la production redevienne opérationnelle rapidement.
- Savoir gérer la communication interne et externe.