CI CROISSANCE INVESTISSEMENT

Formation Cybersécurité

contact@croissance-investissement.com

Tel: 06 64 83 14 43

Actualités Cybersécurité

www.croissanceinvestissement.com

L'année 2020 aura marqué l'histoire en étant l'année de la cybercriminalité, activité illégale ou irrégulière réalisée à travers le cyberespace.

Appréhendez les différents moyens utilisés par les cybercriminels pour exploiter les vulnérabilités de votre système d'information et qui compromettent ainsi vos données sensibles.

Nos formations

- Les menaces du cyber-espace
- Le vocabulaire de la cyber-espace
- Protection des données personnelles
- Bien identifier l'information stratégique à protéger
- Ransomware, comment s'en protéger?
- Se protéger contre les cybercriminels
- Se défendre dans le monde numérique
- Développer sa cybercompétitivité
- Evoluer dans le monde numérique
- Se préparer à une cybercrise
- Référent cybersécurité
- Intelligence économique
- les enjeux de la cybersécurité
- ISO et politiques de sécurité

Toutes nos formations sont prises en charge totalement par votre OPCO.
Pour toute question relative à l'organisation des formations, ou à leur prise en charge, n'hésitez pas à nous interroger
au 06 64 83 14 43 ou contact@croissance-investissement.com

Séminaire
2 heures, incluant une demi-heure d'échange

Les Menaces du Cyber-Espace

- Appréhender les principales menaces informatiques.
- Comprendre les modes opératoires des cybercriminels.
- Connaître les bonnes pratiques de protection.

Les Menaces du Cyber-Espace

1- Comprendre le contexte

- Qu'est-ce qu'une identité numérique ?
- Pourquoi le RGPD ? Rappel du rôle de la CNIL
- Qu'est-ce qu'une donnée à caractère personnel, une donnée sensible selon la CNIL ?

2- Les bonnes pratiques au quotidien

- Comprendre ce qu'est un risque en cybersécurité : Vulnérabilités / Menace / Impacts
- Qu'est-ce que l'ingénierie sociale ?
- Reconnaître un phishing/vishing demandant des données personnelles
- La gestion des mots de passe La veille sur votre identité numérique
- Autres recommandations dans la vie professionnelle : conservation des données, cloisonnement ...

3- Fuite de donnée, que faire ?

- Je suis victime d'une fuite ou d'une attaque sur mon identité numérique : porter plainte / déclaration à la CNIL
- Mon entreprise est victime d'une fuite de données : les premiers gestes, gestion des cyber-crises (cellule de crise, plan de communication)
- Que dit la loi ?

4- Conclusion

Les thèmes complémentaires

Bibliographie

QCM Questions-réponses

Les Menaces du Cyber-Espace

Séminaire
2 heures, incluant une demie-heure d'échange

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS :
QCM collectif de 5 questions à la fin de séance

TARIF
Nous consulter pour devis personnalisé.

Les experts qui animent la formation sont des spécialistes des matières abordées.

Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
3 heures 30, incluant
une 1/2 heure d’échange

Le Vocabulaire de la Cybersécurité

- Connaître les principales menaces informatiques.
- Comprendre l’utilité des principales solutions de sécurité.

Le Vocabulaire de la Cyber-sécurité

1- Introduction

- Les principaux éléments de langage
- Qu'est-ce que l'identité numérique ?
- DCP, Données sensibles et l'importance de cartographier les données numériques
- Le principe de « sécurité » en informatique
- Le contexte légal

2- Les menaces

- Les principales menaces et leurs motivations
- Les principales formes d'attaques

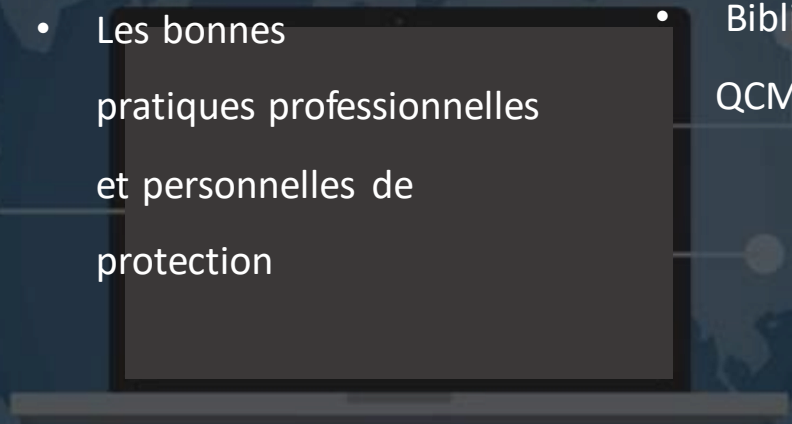
3- Les protections

- Les outils de base de la protection numérique
- Les bonnes pratiques professionnelles et personnelles de protection

4- Conclusion

- Les thèmes complémentaires
- Bibliographie

QCM Questions-réponses



Pare-feu, Deep-Packet-Inspection, SIEM, IDS, Chiffrement, Hachage …. autant de termes utilisés au quotidien par les médias ou vos collaborateurs/prestataires et dont le sens peut vous échapper.

Ce séminaire de 2 heures et demie vous proposera un panorama du vocabulaire de la cybersécurité.

Le Vocabulaire de la Cyber-sécurité

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

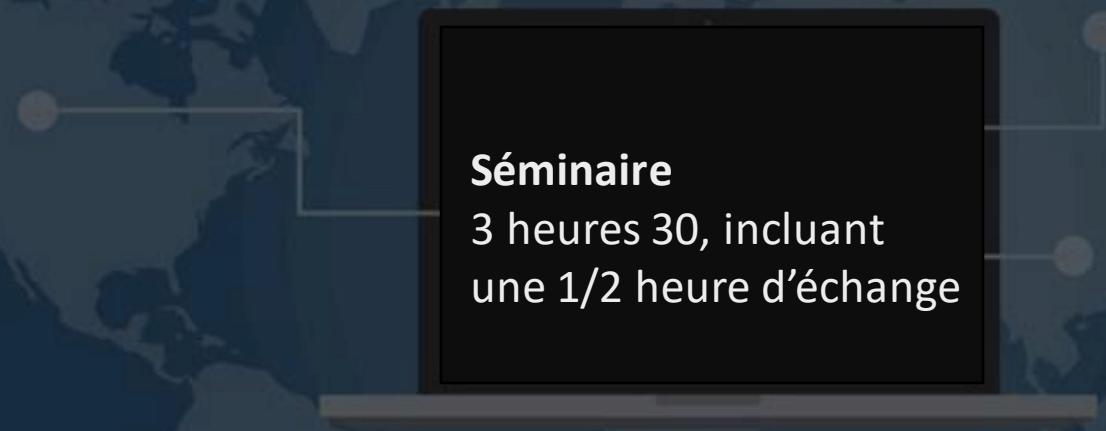
PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 5 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.



Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
2 heures, incluant une demie-heure d'échange

Protection des Données Personnelles

Comprendre ce qu'est l'identité numérique et les risques liés, est pratiques à mettre en œuvre au quotidien, dans sa vie personnelle et professionnelle pour protéger ses données et les gestes essentiels en cas de fuite de données.

Protection des Données Personnelles

1- Comprendre le contexte

- Qu'est-ce qu'une identité numérique ?
- Pourquoi le RGPD ?
- Rappel du rôle de la CNIL
- Qu'est-ce qu'une donnée à caractère personnel, une donnée sensible selon la CNIL ?

2- Les bonnes pratiques au quotidien

- Comprendre ce qu'est un risque en cybersécurité : Vulnérabilités / Menace / Impacts
- Qu'est-ce que l'ingénierie sociale ?
- Reconnaître un phishing/vishing vous demandant des données personnelles
- La gestion des mots de passe
- La veille sur votre identité numérique
- Autres recommandations dans la vie professionnelle : conservation des données, cloisonnement ...

3- Fuite de donnée, que faire ?

- Je suis victime d'une fuite ou d'une attaque sur mon identité numérique : porter plainte / déclaration à la CNIL
- Mon entreprise est victime d'une fuite de données : les premiers gestes, gestion des cyber-crises (cellule de crise, plan de communication)
- Que dit la loi ?

4- Conclusion

- Les thèmes complémentaires
- Bibliographie
- QCM
- Questions-réponses

Protection des Données Personnelles

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 5 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Séminaire
2 heures, incluant une demie-heure d'échange

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent.

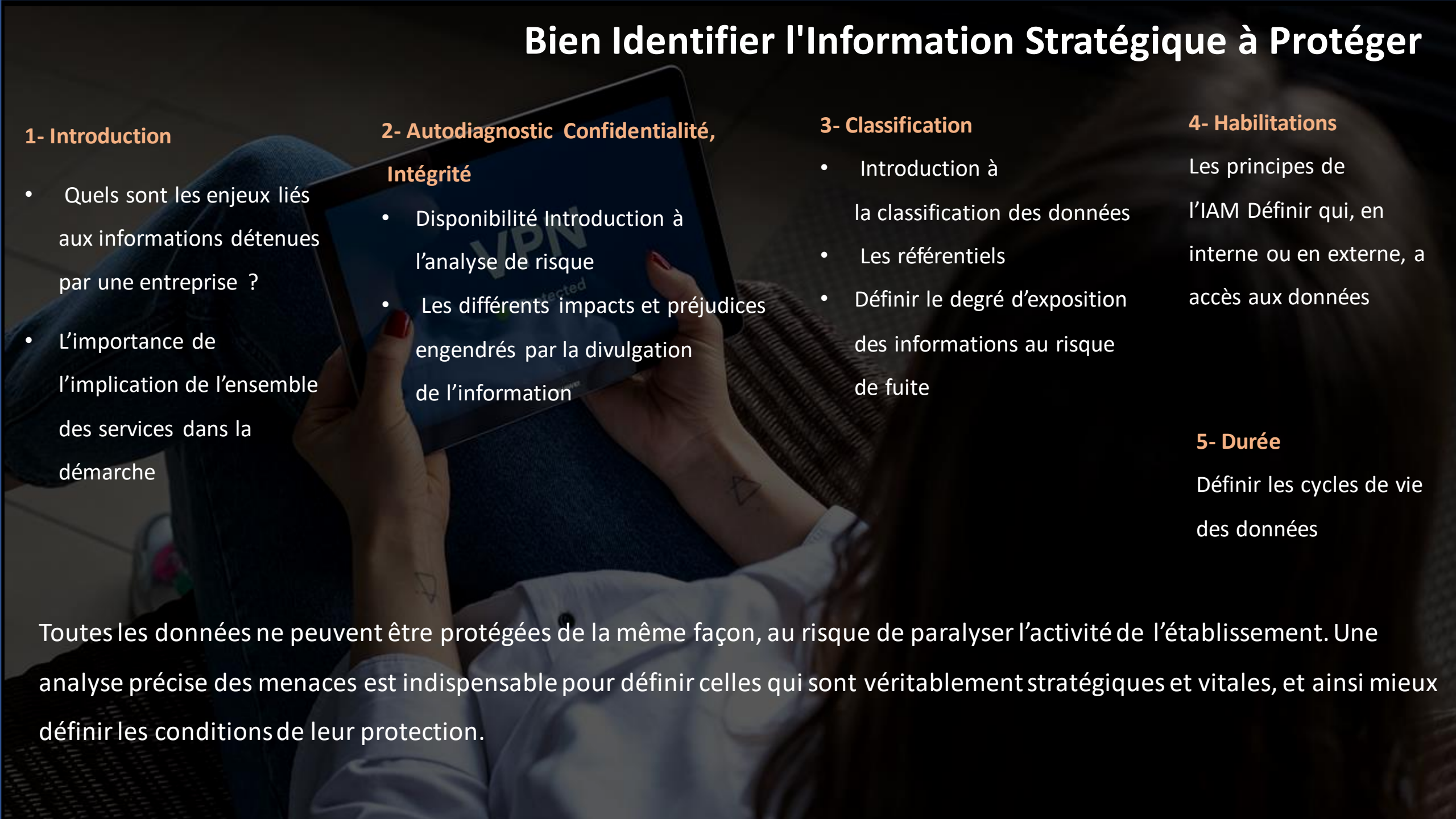
Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
2 heures 30, incluant une 1/2 heure d’échange

Bien Identifier l'Information Stratégique à Protéger

- Comprendre les enjeux liés aux informations détenues par votre entreprise.
- Initier une démarche de protection de l’information stratégique.

Bien Identifier l'Information Stratégique à Protéger



1- Introduction

- Quels sont les enjeux liés aux informations détenues par une entreprise ?
- L'importance de l'implication de l'ensemble des services dans la démarche

2- Autodiagnostic Confidentialité, Intégrité

- Disponibilité Introduction à l'analyse de risque
- Les différents impacts et préjudices engendrés par la divulgation de l'information

3- Classification

- Introduction à la classification des données
- Les référentiels
- Définir le degré d'exposition des informations au risque de fuite

4- Habilitations

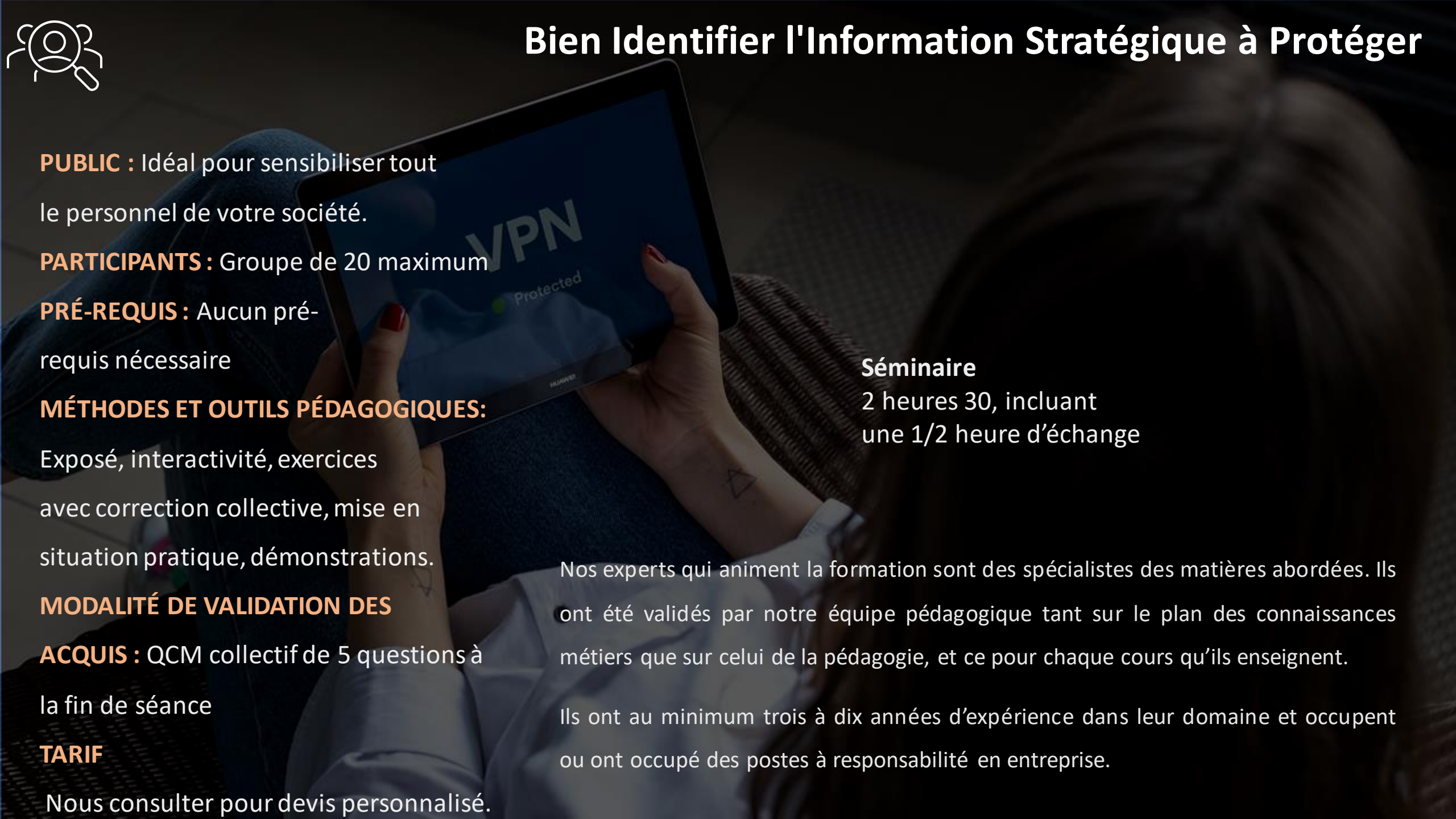
Les principes de l'IAM Définir qui, en interne ou en externe, a accès aux données

5- Durée

Définir les cycles de vie des données

Toutes les données ne peuvent être protégées de la même façon, au risque de paralyser l'activité de l'établissement. Une analyse précise des menaces est indispensable pour définir celles qui sont véritablement stratégiques et vitales, et ainsi mieux définir les conditions de leur protection.

Bien Identifier l'Information Stratégique à Protéger



PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

PRÉ-REQUIS : Aucun pré-requis nécessaire

MÉTHODES ET OUTILS PÉDAGOGIQUES:

Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 5 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Séminaire
2 heures 30, incluant
une 1/2 heure d'échange

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
2 heures 30,
incluant une 1/2 heure
d’échange

Ransomware: Comment s'en Protéger

- Comprendre le mode opératoire d’un ransomware
- Connaître les bonnes pratiques pour s’en prémunir
- Connaître les gestes essentiels en cas d’attaque réussie

Ransomware: Comment s'en Protéger?

1- Comprendre ce qu'est un ransomware

- Qu'est-ce que le chiffrement ?
- Qu'est-ce qu'un logiciel malveillant ?
- Les grandes étapes d'une attaque informatique Ramsomware : mode opératoire, les vulnérabilités exploitées par les ransomwares

2- Se prémunir des ransomwares

- Comprendre ce qu'est un risque en cybersécurité : Vulnérabilités / Menace / Impacts Cartographie du SI / Inventaire des données numériques dans l'entreprise, classement par sensibilité
- Veille (CVE…) et mises à jour : pourquoi, quand, comment ?
- Cloisonnement SI (réseau, utilisateur...)
- Reconnaître un phishing contenant un logiciel malveillant
- Les bonnes pratiques pour partager un fichier PCA/PRA et plans de sauvegarde Antivirus / EDR / Firewall / Proxy / Durcissement des configurations

3- Que faire en cas de cyber-crise

- L'importance de la détection
- Processus de gestion d'incident (comment je gère un incident, comment je sais si c'est grave ?)
- Les premiers gestes Gestion des cyber-crises (cellule de crise, plan de communication, déclencher mon PCA)
- Que dit la loi ?
- Le rôle de l'ANSSI / porter plainte / déclaration à la CNIL
- Payer

4- Conclusion

- Les thèmes complémentaires
- Bibliographie QCM
- Questions-réponses

Ransomware: Comment s'en Protéger?

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS

PÉDAGOGIQUES: Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 5 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Clique ici pour ajouter du texte

Séminaire
3 heures 30, incluant
une 1/2 heure d'échange

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
1/2 jour, soit 4 heures

Se Protéger Contre les Cybercriminels

- Être capables d'évaluer un risque informatique simple.
- Appréhender des principes simples pour limiter ses vulnérabilités.
- Connaître les bonnes pratiques de protection.

Se Protéger Contre les Cybercriminels

1- Introduction

- Définitions et bref historique
- Les principaux éléments de langage
- Les principales composantes du monde numérique Le principe de « sécurité » en informatique

2- Les menaces

- Les principales menaces et leurs motivations
- Les principales formes d'attaques

Le panorama des menaces, passé, présent et à venir

Cliquez pour ajouter du texte

3- La notion de risque

- Les actifs matériels et immatériels
- Les différents types d'impact
- Une méthode simple d'évaluation

4- Les protections

- La limitation de la « surface d'attaque »
- L'optimisation de l'objectif de sécurité

Les outils de base de la protection numérique

- Les bonnes pratiques

de protection professionnelles et personnelles

5- Conclusion

- Thèmes complémentaires
- Bibliographie
- QCM Questions-réponses

Se Protéger Contre les Cybercriminels

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 20 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 5 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Séminaire
1/2 jour, soit 4 heures

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
1 jour, soit 7 heures

Se Défendre dans le Monde Numérique

- Appréhender les principales menaces informatiques
- Comprendre les bmodes opératoires des cybercriminels
- Connaître les bonnes pratiques de protection

Se Défendre dans le Monde Numérique

1- Introduction

- Définitions et bref historique
- Les principaux éléments de langage
- Les principales composantes du monde numérique
- Le principe de « sécurité » en informatique
- Les principaux acteurs du monde numérique

2- Les menaces

- Les principales menaces et leurs motivations
- Les principales formes d'attaques
- Le panorama des menaces, passé, présent et à venir

3- Le risque

- La notion de risque
- Les actifs matériels, professionnels et personnels, le cas du BYOD
- Les actifs immatériels, le cas des médias sociaux
- Les types de risques
- Les différents types d'impact
- Les aspects juridiques : les infractions et les responsabilités
- Les principales méthodes d'évaluation des risques

4- Les protections

- La limitation de la « surface d'attaque »
- L'optimisation de l'objectif de sécurité
- Les outils de protection des données, des systèmes et des communications
- Le principe du chiffrement et de la signature numérique
- Les bonnes pratiques professionnelles et personnelles de protection

5- Réagir

- L'utilisation de la preuve numérique
- La procédure pénale, commerciale et civile Les acteurs de la réaction, les cas de l'atteinte à l'image, de l'usurpation

6- Conclusion

- Les thèmes complémentaires
- Bibliographie
- QCM Questions-réponses

Se Défendre dans le Monde Numérique

Séminaire
1 jour, soit 7 heures

PUBLIC : Idéal pour sensibiliser tout le personnel de votre société.

PARTICIPANTS : Groupe de 8 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 10 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
1 jour, soit 7 heures

Se Préparer à une Cybercrise

Développer une culture de la gouvernance de crise dans le contexte du cyberespace et face aux enjeux de la cybersécurité.

Se Préparer à une Cybercrise

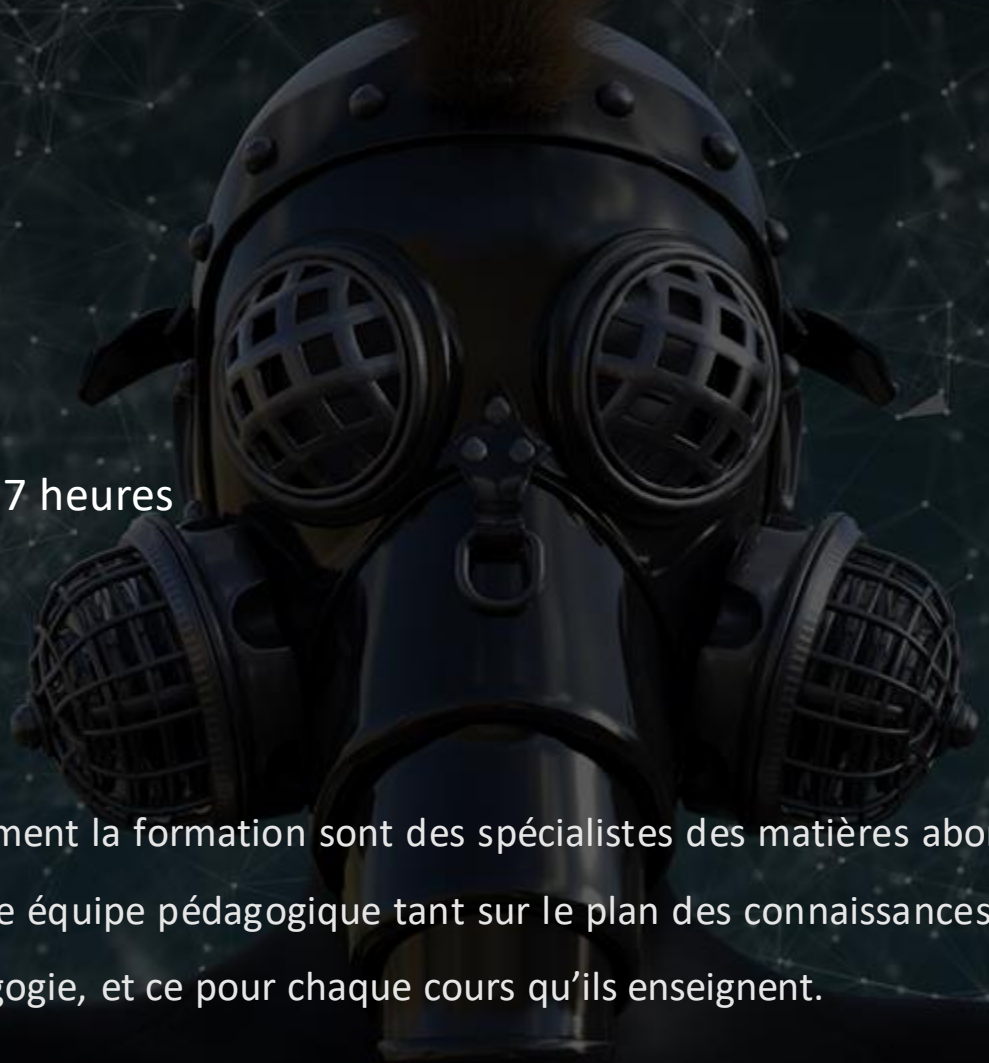
1- Les différentes méthode

- Définition événement, incident et crise
- Les référentiels
- Les différentes cellules
- Réponse de Sécurité globale
- Méthodologie 4PCR : Prévision, Prévention, Préparation, Protection, Continuité, Résilience

2- Déploiement de la méthode Prévision : systèmes de prévisions et de surveillances, recherches scientifiques et procédés technologiques.

- Prévention : connaissance des risques, prise en compte dans l'aménagement, surveillance, mesures et dispositifs visant à réduire l'aléa ou ses effets (Mitigation).
- Préparation : information et formation des acteurs permanents et des collaborateurs occasionnels, des sous-traitants, des fournisseurs et des clients, des milieux professionnels, du citoyen et du système éducatif.
- Protection : dispositifs d'alerte, plans de secours, guide méthodologique, fiches réflexes, cellules de crise, organisation de gestion de crise.
- Continuité : organisation en mode dégradée, plan de continuité d'activités.
- Résilience : capacité à retrouver son état initial, à dépasser la crise, retex et amélioration continue.

Se Préparer à une Cybercrise



PUBLIC : Dirigeant, RSSI, RPCA/RPRA

PARTICIPANTS : Groupe de 8 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES: Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 10 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Séminaire
1 jour, soit 7 heures

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
2 jours, soit 14 heures

Evoluer dans le Monde Numérique

- **Connaître les principales menaces informatiques, les modes opératoires des cybercriminels et les bonnes pratiques de protection.**
- **Être capables d'évaluer un risque informatique simple, de réagir face à une attaque informationnelle et de piloter des procédures numériques.**
- **Comprendre l'utilité des principales solutions de sécurité.**

Evoluer dans le Monde Numérique

JOURNÉE 1

MATIN

1- Introduction

Définitions et bref historique - Les principaux éléments de langage. Les principales composantes du monde numérique Le principe de « sécurité » en informatique Les principaux acteurs du monde numérique

2- Les menaces Les principales menaces et leurs motivations - Les principales formes d'attaques - Le panorama des menaces, passé, présent et à venir

APRÈS-MIDI

3- Le risque

La notion de risque Les actifs matériels, professionnels et personnels, le cas du BYOD - Les actifs immatériels, le cas des médias sociaux - Les types de risques - Les différents types d'impact Les aspects juridiques : les infractions et les responsabilités - Les principales méthodes d'évaluation des risques

JOURNÉE 2

MATIN

4- Les protections

La limitation de la « surface d'attaque » L'optimisation de l'objectif de sécurité - Les outils de protection des données, des systèmes et des Communications - Le principe du chiffrement et de la signature numérique - Les bonnes pratiques professionnelles et personnelles de protection

APRÈS-MIDI

5- L'investigation

L'utilisation de la preuve numérique - La procédure pénale, commerciale et civile L'investigation numérique, son intérêt et les conditions de sa mise en œuvre - La perquisition numérique - Le panorama des acteurs - Les techniques et outils de recherche de preuves numériques - Le cas de la mobilité, du cloud, du chiffrement - L'actualité juridique

6- Conclusion

Les thèmes complémentaires - Bibliographie - QCM - Questions-réponses

Evoluer dans le Monde Numérique

PUBLIC : Dirigeant, RSSI, RPCA/RPRA

PARTICIPANTS : Groupe de 8 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 10 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Séminaire
2 jours, soit 14 heures

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
2 jours, soit 14 heures

Développer sa Cybercompétitivité

- Développer une culture du management de l'information stratégique et de la gouvernance de crise dans le contexte du cyberespace et face aux enjeux de la cybercompétitivité.

Développer sa Cybercompétitivité

JOURNÉE 1

MATIN

1- Le cyber-espace et la cybercompétitivité

Définitions - Présentation de la méthode Menaces, vulnérabilités et opportunités - Préconisations nationales (stratégie nationale de sécurité numérique) et internationale

APRÈS-MIDI

2- Évaluer sa maturité numérique

Définition du SI, du SMSI, documentation … - Méthode d'évaluation en termes de vulnérabilités et d'opportunités - Mesurer sa compétitivité (prix et hors prix) - Mesurer sa capacité à évoluer durablement dans leur environnement.

JOURNÉE 2

MATIN

3- Les domaines d'action de la méthode

Avantage compétitif et concurrentiel Vie numérique - Synergie et influence territoriale - Gouvernance de crise - Responsabilité sociale et environnementale

APRÈS-MIDI

4- La méthode Les acteurs concernés

Modification des usages et des pratiques des acteurs concernés - Modification des comportements des individus Évolution de l'organisation de la structure - Engagement Processus de management considérationnel - L'importance de la communication

Développer sa Cybercompétitivité

Séminaire
2 jours, soit 14 heures

PUBLIC : Dirigeant, RSSI, RPCA/RPRA

PARTICIPANTS : Groupe de 8 maximum

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations.

MODALITÉ DE VALIDATION DES ACQUIS : QCM collectif de 10 questions à la fin de séance

TARIF

Nous consulter pour devis personnalisé.

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
4 jours ouvrés
temps plein

Référent Cybersécurité

- Référent cybersécurité : pour les entreprises qui veulent créer une fonction dans l'entreprise

Référent Cybersécurité

Objectifs :

- Maîtriser les enjeux de la cybersécurité pour l'entreprise
- Sensibiliser à l'importance d'une politique de sécurité des systèmes d'information (SSI) au sein d'une TPE/PME
- Identifier les menaces liées à l'utilisation de l'informatique et des réseaux Internet
- Présenter les précautions techniques et juridiques pour faire face aux attaques.

Thèmes :

- La cybersécurité et les enjeux de la SSI : nouvelle économie de la cybercriminalité, vulnérabilités des systèmes d'information
- Cartographie des systèmes d'informations de l'entreprise – analyse des risques : politique de SS*I (B*yod et externalisation)
- Hygiène informatique pour les utilisateurs : identifier le patrimoine informationnel de son ordinateur, maîtriser les réseaux informatiques : Intranet/Internet, mots/phrases de passe, etc.
- Dispositifs de prévention en matière de sécurité économique et gestion de crise SSI (veille et alerte, plans de continuité/plans de reprise d'activité).

Référent Cybersécurité

Séminaire
4 jours ouvrés temps plein

PUBLIC : dirigeants, cadres de TPE/PME/ETI

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES: Exposé, interactivité, mise en situation pratique, démonstrations.

TARIF

4 680 euros HT

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
3 jours
ouvrés temps plein

Intelligence Economique

- Intelligence économique, propriété intellectuelle et empreinte numérique de l'entreprise

Intelligence Economique

Objectifs :

- Maîtriser les enjeux de la cybersécurité pour l'entreprise
- Sensibiliser à l'importance d'une politique de sécurité des systèmes d'information (SSI) au sein d'une TPE/PME
- Identifier les menaces liées à l'utilisation de l'informatique et des réseaux Internet
- Présenter les précautions techniques et juridiques pour faire face aux attaques.

Thèmes :

- La cybersécurité et les enjeux de la SSI : nouvelle économie de la cybercriminalité, vulnérabilités des systèmes d'information
- Cartographie des systèmes d'informations de l'entreprise – analyse des risques : politique de SSI *(B*yod et externalisation)
- Hygiène informatique pour les utilisateurs : identifier le patrimoine informationnel de son ordinateur, maîtriser les réseaux informatiques : Intranet/Internet, mots/phrases de passe, etc.
- Dispositifs de prévention en matière de sécurité économique et gestion de crise SSI (veille et alerte, plans de continuité/plans de reprise d'activité).

Intelligence Economique

PUBLIC : dirigeants, cadres de TPE/PME/ETI

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, mise en situation pratique, démonstrations.

TARIF

3 515 euros HT

Séminaire
3 jours ouvrés temps plein

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
3 jours
ouvrés temps plein

ISO et politiques de Sécurité

Comment concilier productivité et sécurité?

ISO et Politiques de Sécurité

Objectif

- Standardiser la gestion de projet basé sur les processus et l'amélioration continue (méthodes et outils)
- Sécurité des systèmes et de l'information dans la chefferie de projets (méthode, standards ISO et outils)
- Implémentation opérationnelle pour l'organisation

Thèmes principaux

- Méthodologies de gestion de projets, de la qualité IT et de la sécurité
- Ingénierie informatiques et gestion des processus
- Standards et outils d'implémentation de la conduite du changement
- Outils et mesures de la performance (Devops, Leant IT, Prince 2)

ISO et Politiques de Sécurité

PUBLIC : Dirigeants, cadres de directions et cadres opérationnels, chefs de projets des secteurs publics et privés
Professions libérales

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS PÉDAGOGIQUES : Exposé, interactivité, mise en situation pratique, démonstrations.

TARIF

3 515 euros HT

Séminaire
3 jours ouvrés temps plein

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Séminaire
3 jours ouvrés temps plein

Les Enjeux de la Cybersécurité

Comment concilier productivité et sécurité

Les Enjeux de la Cybersécurité

Objectifs :

- Former aux risques d'intrusions provenant de puissances ou d'intérêts extérieurs, auxquels les acteurs peuvent être confrontés dans leur activité
- Présenter les réponses défensives et offensives prévues au niveau gouvernemental pour contrer ces menaces
- Sensibiliser à l'importance d'une politique de Sécurité des systèmes d'information (SSI).
- Propriété intellectuelle et noms de domaine

Thèmes :

- Les dispositifs de prévention en matière de sécurité économique (DGSI)
- Les intrusions sur les systèmes d'information et de communication, les cas de cybercriminalité (DGSI)
- La protection du patrimoine industriel et économique (DRSD)
- La sécurité des systèmes d'information et de communication (ANSSI)
- Organisation des services de renseignement (DGSE)
- Retex d'entreprises (sécurité économique, SSI).

Les Enjeux de la Cybersécurité

PUBLIC : dirigeants, cadres de TPE/PME/ETI

PRÉ-REQUIS : Des connaissances générales sur l'informatique et le réseau Internet sont recommandées.

MÉTHODES ET OUTILS

PÉDAGOGIQUES: Exposé, interactivité, mise en situation pratique, démonstrations.

TARIF
4 680 euros HT

Séminaire
3 jours ouvrés temps plein

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

contact@croissance-investissement.com
Tel: 06 64 83 14 43

Actualités Cybersécurité

www.croissanceinvestissement.com

CI CROISSANCE INVESTISSEMENT