VOTRE FORMATION

LE LIEU

La formation se déroulera en présentiel à Saint-Barthélemy

CONTACTS

CHAMBRE ECONOMIQUE
MULTIPROFESSIONNELLE
Établissement Public Territorial
de la Collectivité de Saint-Barthélemy
57 chemin des Sables - Saint Jean
97133 Saint-Barthélemy
Tél. : 05 90 27 12 55
formation@cemstbarth.com
www.cemstbarth.com

Siret : 130 004 708 00033
N° d'activité: 95 9700165497

GG - Version 03 - 01/01/2022

CHAMBRE ECONOMIQUE
MULTIPROFESSIONNELLE
Saint-Barthélemy

SE PERFECTIONNER EN CYBERSÉCURITÉ

LA FORMATION

Cette formation de 14h permet d'approfondir ses connaissances en cybersécurité et de faire face aux menaces avancées.

Elle aborde les aspects stratégiques (gouvernance, cadre réglementaire, RGPD) et opérationnels (outils collaboratifs, mobiles, gestion des accès).

Les participants apprennent à anticiper et gérer une crise grâce à des méthodes et outils éprouvés.
Des ateliers pratiques et mises en situation réalistes renforcent l'acquisition des compétences.

Un programme complet pour renforcer la résilience numérique des organisations et des équipes.

LES OBJECTIFS

- Approfondir ses connaissances en cybersécurité afin de mieux protéger son organisation face aux menaces avancées.
- Comprendre le cadre réglementaire et les obligations légales liées à la protection des données.
- Développer des compétences opérationnelles pour sécuriser ses outils numériques et réagir efficacement en cas d'incident.

MÉTHODES ET OUTILS PÉDAGOGIQUES

OUTILS

- Salle adaptée pour recevoir une formation, paperboard, moyens audiovisuels appropriés aux sujets traités, diaporamas, vidéo, PowerPoint
- Le formateur s'appuiera sur des cas pratiques, exercices et exemples concrets
- Ordinateur portable et connexion internet

MÉTHODE

Formation interactive, basée sur une présentation du formateur, des échanges avec les stagiaires et des mises en situation via des cas pratiques.

PROFIL FORMATEUR

Tous les formateurs répondent aux exigences des cahiers des charges dont l'expérience professionnelle et les diplômes ont été validés.

PROGRAMME

CHAMBRE ECONOMIQUE MULTIPROFESSIONNELLE
Saint-Barthélemy

La formation de vos projets commence ici....

PUBLIC CONCERNÉ

Cette formation s'adresse aux professionnels ayant déjà acquis les bases de la cybersécurité.

Elle est particulièrement adaptée aux managers, responsables de service, référents sécurité, responsables informatiques, informaticiens et collaborateurs manipulant des données sensibles.

Elle convient aux organisations souhaitant renforcer leur niveau de protection, sécuriser leurs outils collaboratifs et être prêtes à réagir efficacement en cas d'incident.

PRÉ REQUIS

- Maîtriser la langue française à l'oral et à l'écrit
- Avoir suivi une formation d'initiation à la cybersécurité ou disposer de connaissances de base sur les bonnes pratiques numériques (gestion des mots de passe, vigilance face aux mails suspects, mises à jour, etc.)
- Être à l'aise avec l'usage quotidien des outils numériques (ordinateurs, smartphones, outils collaboratifs)

PROGRAMME

APPROFONDISSEMENTS & CADRE STRATÉGIQUE

1. PANORAMA DES MENACES AVANCÉES ET IMPACTS SUR LES ORGANISATIONS

- Analyse des attaques ciblées (spear phishing, ransomware, APT, supply chain)
- Nouveaux vecteurs : IoT, cloud, applications collaboratives
- Études de cas d'incidents récents et analyse de leurs impacts (juridiques, financiers, réputationnels)

2. GOUVERNANCE ET CADRE RÉGLEMENTAIRE

- Principes du RGPD liés à la cybersécurité et à la protection des données
- Obligations légales des entreprises : conservation, notification d'incident, responsabilité
- Mise en place d'une gouvernance interne de la sécurité (rôles, sensibilisation, politique interne)
- Panorama des normes et référentiels (ISO 27001, ANSSI, NIST)

3. ATELIERS PRATIQUES

- Cartographie des risques numériques d'une organisation
- Diagnostic rapide de maturité cybersécurité
- Cas pratique : analyser une attaque et identifier les failles exploitées

PROTECTION OPÉRATIONNELLE & GESTION DE CRISE

4. PROTECTION DES OUTILS COLLABORATIFS ET MOBILES

- Sécurisation des environnements collaboratifs (Microsoft 365, Google Workspace, Slack...)
- Gestion des accès, droits et authentification forte
- Sécurité des terminaux mobiles : BYOD, applications, Wi-Fi publics
- Outils et solutions de protection (EDR, MDM, etc.)

5. GESTION DE CRISE ET RÉPONSE AUX INCIDENTS

- Processus de gestion de crise : détection, confinement, éradication, reprise
- Organisation d'une cellule de crise et rôles associés
- Communication en situation d'incident (interne, externe, autorités)
- Exercices de continuité d'activité et plan de reprise (PCA/PRA)

6. MISE EN SITUATION & ATELIERS PRATIQUES

- Simulation d'incident (cyberattaque fictive) : réagir en temps réel
- Élaboration d'un plan de gestion de crise adapté au secteur des participants
- Atelier collectif : construire un plan d'action cybersécurité pour son organisation

DURÉE
La formation dure 14h00 soit 2 jours.

MÉTHODE D'ÉVALUATION

Cette formation n'est pas soumise à une évaluation.

FINALITÉ

- Attestation de fin de formation

Cette formation fait l'objet d'une mesure de satisfaction globale des stagiaires rentrant dans le cadre de la certification Qualiopi de l'établissement.

LE COÛT & LA DATE

La tarification et la date sont disponibles sur notre site Internet. N'oubliez pas qu'il existe différents systèmes de financement de vos actions de formation. Le Centre de Formation vous accompagne dans vos démarches.

Formation adaptable aux personnes en situation de handicap. Veuillez contacter la référente handicap Alexia Louis au 05 90 27 12 55 ou par mail à : alexia.louis@cemstbarth.com

POUR VOUS INSCRIRE, NOUS VOUS INVITONS À COMPLÉTER LE BULLETIN D'INSCRIPTION SUR LE SITE INTERNET DE LA CEM : WWW.CEMSTBARTH.COM