le cnam
Bretagne

CYBER

FORMATIONS COURTES

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE
Liberté
Égalité
Fraternité

Région
BRETAGNE

À l'ère numérique actuelle, la sécurité informatique est cruciale pour toute organisation. C'est pourquoi le Cnam Bretagne a développé des programmes de formation de haute qualité de courte durée, pour répondre aux besoins de votre entreprise.

Nos formations sont adaptées à différents niveaux de compétences, et elles couvrent une gamme complète de sujets, de la prévention des cybermenaces à la conformité RGPD en passant par la sécurisation des postes informatiques.

RBOE01

PRÉVENTION EN CYBERSÉCURITÉ
RISQUES ET BONS USAGES

Objectifs de la formation

Les usages numériques ont particulièrement évolué avec le recours au télétravail, l'utilisation de nombreux services et objets connectés. Ce contexte a favorisé le développement et la fréquence des cyberattaques de plus en plus professionnalisées. Tout salarié est naturellement confronté à ces menaces, car il est la 1ere porte d'entrée dans le système d'information de l'entreprise.
Cette formation consiste à former vos salariés à la compréhension de la cybermenace afin qu'ils acquièrent de bonnes pratiques et améliorent la protection des données de l'entreprise.

Cas d'usage

- Identifier les enjeux personnels et professionnels en cybersécurité
- Auto-analyser ses pratiques de sécurité
- Comment avoir un mot de passe solide ?
- Commenter et utiliser un coffre-fort numérique pour stocker tous ses mots de passe
- Comment reconnaître les pièges du phishing ?
- Comment se protéger d'une usurpation d'identité ?
- Comment se prémunir contre les fuites de données personnelles ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

3h30
en présentiel ou distanciel (en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

Prérequis
aucun

nombre de places mini.
5 personnes

tout public ayant accès à un système d'information (niveau débutant)

445 €
par participant

222,50 €
Tarif EDIH par participant

Programme

Mot de passe
- Temps de résistance d'un mot de passe, autotest
- Vol de mot de passe : risques encourus pour le salarié/son entreprise
- Créer et gérer ses mots de passe : solidité, longueur, diversité, confidentialité
- Utiliser un coffre-fort numérique pour stocker tous ses mots de passe

Hameçonnage ou « phishing »
- La technique du hameçonnage : exemples
- Pourquoi les données intéressent-elles les pirates ?
- Comment reconnaître les pièges ?
- Que faire si l'on est piégé ?

Usurpation d'identité
- Quelle définition ?
- Les conséquences d'une usurpation d'identité suite à un hameçonnage
- Comment s'en protéger ?
- Les peines encourues

Fuite de données
- Qu'est-ce qu'une fuite ou violation de données personnelles ?
- Comment se prémunir contre les fuites de données personnelles ?
- Que faire en cas de fuite ou violation de données personnelles ?
- Violation de données personnelles, les types d'infractions

RBOE02

SÉCURITÉ INFORMATIQUE
RISQUES, CONSÉQUENCES ET MESURES DE PROTECTION

Objectifs de la formation

Quelle soit petite ou de grande taille, toute organisation est soumise au risque cyber. La connaissance et la maîtrise de ce risque sont donc incontournables pour éviter une perte d'activité. L'objectif de cette formation est d'identifier et de comprendre les risques cyber, de les mesurer et de déterminer les actions à mettre en œuvre afin de les réduire.

Cas d'usage

- Quels sont les risques cybersécurité pour mon entreprise ?
- Comment réaliser une analyse de risques ?
- Quelles sont les principales mesures de sécurité à mettre en place ?
- Comment structurer son management à la sécurité de l'information (SMSI) ?
- Comment se préparer à une crise de cybersécurité (PCA / PRA) ?

21 h (3 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

2775 €
par participant

1388 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne en charge de la sécurisation d'un système informatique ou souhaitant être sensibilisée à la maîtrise des risques cyber, notamment :
- Directeur
- Responsable du Plan de Continuité d'Activité (RPCA - BCM)
- Chargé de gestion de crise
- Responsable opérationnel
- Responsable de la Sécurité des Systèmes d'Information (RSSI - CISO)

Prérequis
aucun

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

Programme

Introduction
- Référentiel général de sécurité (RGS)
- Principes généraux relatifs à la protection des données de la RGPD

Démarche d'homologation de la sécurité
- Précision du référentiel réglementaire
- Délimitation du périmètre
- Diagnostique des besoins de sécurité et du niveau de maturité SSI de l'organisme
- Acteurs de l'homologation

Appréciation des risques
- Approche et limites de l'analyse des risques
- Cadre de l'analyse de risques (ISO 27005 :2018)
- NIST SP 800 30
- MEHARI
- ANSSI EBIOS Risk Manager
- Analyse d'impact relative à la protection des données (Privacy Impact Assessment)
- Analyse de la maturité du SI

Focus sur EBIOS Risk Manager

Périmètre de contrôle et audits

Décision formelle d'homologation

Plan de traitement des incidents et de reprise d'activité
- Principes généraux
- Introduction à la mise en œuvre d'un PCA / PRA (basé sur la norme ISO 22301)
- Procédure d'alertes et de gestion de crise

La maintenance et le suivi de la sécurité des systèmes d'information
- Mise en place d'une démarche d'amélioration continue basée sur la norme ISO 27001
- Veille technique et juridique de la sécurité des systèmes d'information

RBOE03

RGPD
RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Objectifs de la formation

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. Tous les organismes sont aujourd'hui touchés par des attaques, quels que soient leur taille et leur secteur. Ces attaques relèvent de la cybermenace et ont des finalités variées allant de l'espionnage au sabotage et passant par la déstabilisation et le profit financier.
Cette formation vise à enseigner par des exemples concrets les principales mesures qu'il convient de mettre en place pour la protection des données.

Cas d'usage

- Quelles sont les contraintes légales de gestion des données pour mon entreprise ?
- Comment initier un chantier RGPD ? Comment structurer ma feuille de route ?
- Comment mettre en œuvre le registre simplifié des traitements ?
- Comment sécuriser mes traitements de données ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne concernée par le traitement de données personnelles (RH, marketing, comptabilité, ...), notamment : DPO, DSI, RSSI, Juriste.

Prérequis
aucun

Programme

Introduction au RGPD
- Genèse du règlement
- Définitions : Données à caractère personnel, Données sensibles, Traitement, Responsable de traitement, Sous-traitant, Délégué à la protection des données
- Principes de licéité des traitements : finalités du traitement, qualité des données, durée de conservation, base juridique de traitement
- Obligations du Responsable de traitement et du Sous-traitant

Feuille de route pour les traitements
- Cartographie : comment identifier les traitements de données personnelles et leurs supports ?
- Cas de l'anonymisation
- Référencement des traitements dans un registre simplifié pour les TPE
  - Atelier exploitant le modèle proposé par la CNIL
- Garantir la sécurité des données : Approche par les risques
  - Atelier mettant en œuvre l'outil PIA de la CNIL

Sécurisation des traitements
- Rappel de l'obligation du Responsable de traitement
- Introduction à la notion de code de conduite
- Cas de l'informatique en nuage
- Revue des 12 règles essentielles de sécurisation de l'informatique applicables à la protection des données personnelles
- Démonstration de génération de mot de passe robuste au moyen de l'outil Keepass
- Atelier mettant en œuvre le guide de la CPME/ANSSI sur des exemples concrets
- Focus sur les mesures de journalisation
- Focus sur la « pseudonymisation »

Que faire en cas de violation des données personnelles ?

RBOE04

SÉCURISER UN PARC INFORMATIQUE
BONNES PRATIQUES

Objectifs de la formation

La transformation numérique des entreprises et collectivités permet d'optimiser des processus et rapprocher les entreprises de leurs clients ou usagers. Mais cette transformation s'accompagne de risques cyber qui ne cessent de s'intensifier. Il faut s'en protéger à tous les niveaux et mettre en place de bonnes pratiques techniques pour sécuriser le système d'information de son entreprise.
Cette formation vise à enseigner par des exemples concrets les principales mesures qu'il convient de mettre en place pour sécuriser ses postes informatiques.

Cas d'usage

- Quels sont les menaces et les risques ?
- Quels sont les principes fondamentaux de sécurité ?
- Comment sécuriser un poste de travail, sa messagerie, gérer le nomadisme, l'usage du cloud ?
- Comment sécuriser la pratique du nomadisme ? La messagerie ? L'usage du Cloud ?
- Comment réagir en cas de cyberattaque (techniquement et légalement) ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne assurant le rôle d'administrateur système ou réseau au sein de sa PME ou ayant un niveau technicien informatique et souhaitant connaître les règles de bases de protection d'un poste informatique.

Prérequis
aucun

Programme

Les bases de la cybersécurité
- Gestion de la sécurité informatique
- La P.S.S.I.
- L'inventaire, les documentations, manuels et charte de sécurité
- Connaître le parc informatique ainsi que les actifs métiers

Sécuriser les postes de travail
- Chiffrement du disque dur avec BitLocker
- L'importance de l'authentification
  - Risque et bonnes pratiques sur les mots de passe
  - Conteneur de mots de passe (KeePass)
  - L'authentification multifacteurs
  - Mise en place d'une authentification par certificats
  - Les demandes d'élévation de privilèges (UAC)
  - Infrastructure de gestion de clés et PKI
- Savoir gérer les autorisations
  - Gestion de politiques de sécurité (ACL)
  - Les applications non désirées (unwanted application)
  - Blocage d'applications (AppLocker)
  - Surveillance et cloisonnement de certaines applications (AppLocker)
- Surveillances des PC
  - La journalisation des évènements
  - Les antivirus (Windows Defender)
- Sécuriser la messagerie
  - Former le personnel au phishing
  - Les logiciels Antivirus / Anti-Spam et anti-phishing
- La gestion des sauvegardes

Sécuriser les réseaux
- Panorama de techniques malveillantes (vol de session, usurpation d'IP, scan réseau, etc.)
- Rappels sur les réseaux
  - @Mac, @IP, Routage, ICMP, DHCP, DNS)
  - Sécurité des protocoles (http, FTP, Telnet, etc.)
  - Segmentation réseau : les VLANs
- Protéger son réseau
  - Filtrer les réseaux avec les Pare-Feu
  - Ruptures de protocoles avec les Proxy
  - Les bastions
  - Les DMZ

Le nomadisme
- Risques d'accès physique
- Les risques des wifi publics et réseaux
- L'usage des VPN (le full-tunneling)

RBOE05

SAVOIR GÉRER UNE CRISE

Objectifs de la formation

Les spécificités liées à la problématique cyber démontrent la nécessité de se préparer à une attaque en formalisant les attaques passées afin d'en reconnaître des « patterns » et en organisant des exercices afin que chaque auditeur puisse en comprendre les enjeux ainsi que le rôle qu'il va devoir jouer sur l'ensemble de la chaîne de sécurité dans le cadre d'une crise cyber.

Cas d'usage

- Comment mettre en place une organisation de prévention et de gestion de crise ?
- Comment réaliser des plans de défense, PRA, PCA, PCI, PRI, fiches réflexes, etc. ?
- Comment identifier les compétences utiles à la gestion de crise et savoir les mobiliser, utiliser au mieux les plans élaborés au fur et à mesure du déroulement du scénario ?
- Comment se coordonner entre les équipes techniques et managériales ?
- Comment rendre compte aux instances étatiques (déclaration d'incident, couverture médiatique) et internes (ensemble des équipes, gouvernance et membres d'autres cellules) ?

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne en charge de la sécurisation d'un système informatique ou souhaitant être sensibilisée à la maîtrise des risques cyber, notamment :
- Directeur
- Responsable du Plan de Continuité d'Activité (RPCA - BCM)
- Chargé de gestion de crise
- Responsable opérationnel
- Responsable de la Sécurité des Systèmes d'Information (RSSI - CISO)

Prérequis
aucun

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

Programme

Introduction au RGPD

Introduction à la modélisation de la menace

Cycle de la Threat Intelligence

Organisation d'une cellule de crise
- Planifications
  - Politique de sécurité, plans de défense, SMCA
  - Continuité d'activité (PCA, PCO, PGC, PRA) et continuité informatique (PCI, PRI)
- Méthodologie de gestion de crise
  - Qu'est-ce qu'une crise ? Typologies de crises
  - Gestion d'incidents et gestion de crise
  - Mécanismes de prise de décisions
- Décisions en situation de crise
  - Étude d'une crise pour en tirer des enseignements
  - Passage en crise : réunion et ordres de déclenchement, mise en configuration de crise, décisions
- Coordonner la communication de crise

Exercice de crise
- Coordonner les équipes
- Réaliser les déclarations légales nécessaires en fonction de la situation simulée et de la législation applicable
- Gérer les phases de réaction immédiate et d'investigation

Rétrospective sur le déroulé de l'exercice
- « Déconfliction » : facteurs, conduite, compte-rendu
- Compte rendu et modélisation de l'attaque effectuée
- Adaptation de l'organisation et des procédures dans un processus d'amélioration continue

RBOE00

LA CYBERSÉCURITÉ
POUR MANAGER ET AVANT-VENTE

En 7 modules de Master Classes et de conférences-débats avec des experts et spécialistes Cyber, plongez dans l'écosystème Cyber pour découvrir ses codes, ses enjeux, ainsi que les technologies et méthodologies sous-jacentes.

Chaque jour la presse se fait l'écho d'attaques et de piratages informatiques, de divulgations d'informations sensibles ou de fragilités découvertes dans les produits et services numériques.

Derrière ces incidents, nous découvrons des menaces, certaines fois complexes, des actions criminelles, étatiques ou activistes. Construire des systèmes sûrs, les protéger et les défendre, dans une société où accélérer la digitalisation est devenu un challenge quotidien pour les équipes spécialisées qui luttent contre ces menaces. La cybersécurité est un domaine de mythes et de légendes. Ses activités plongent au plus profond de notre histoire avec des luttes ancestrales entre le méchant et le gentil, le gendarme et le voleur, le corsaire et le pirate, en n'oubliant pas les luttes secrètes entre les espions et le contre-espionnage. Une thématique qui résonne, donc, comme un domaine de romans et qui se traduit toutefois par une réalité souvent moins réjouissante pour les équipes chargées de la cybersécurité dans les entreprises. Les métiers de la cybersécurité sont nombreux, pour certains très techniques, d'autres plus fonctionnels, juridiques, ou managériaux. Pour mieux comprendre cet univers, il faut l'explorer sous toutes les facettes ...

7 modules de 5h
en e-learning et visioconférence

3000 €
par participant

1500 €
Tarif EDIH par participant

Prochaine session :
Contacter nos conseillers

Manager et avant-vente souhaitant comprendre l'environnement de la cybersécurité.

Prérequis
aucun

nombre de places mini.
5 personnes

Objectifs de la formation

- Contexte & environnement : s'exprimer dans le même langage que les acteurs du domaine
- Les risques numériques : déterminer les évènements redoutés de l'entreprise
- Architecture & Technologies : appréhender la complexité de l'environnement cyber d'une entreprise
- Management de la sécurité : appréhender les enjeux de conformité et de pilotage d'une entreprise
- La sécurité opérationnelle : s'avoir s'insérer dans l'organisation de la cyberdéfense française
- La sécurité dans les projets : la sécurité dans les projets et la sécurité de l'entreprise
- Le business de la sécurité : se positionner dans l'écosystème cyber du marché

RBOE00

LA CYBERSÉCURITÉ
POUR MANAGER ET AVANT-VENTE

Programme

1. Contexte et environnement (2x1h de e-learning, 1h30 de conférence)
- Petite histoire de la cybersécurité
- Les cybermenaces et leurs auteurs
  - La dure réalité du numérique (exemples marquants)
  - Attaquants : la réalité de la cybercriminalité, et de la Cyberguerre
  - Types et vecteurs d'attaques
  - Darkweb et Darkbusiness
- L'entreprise face au numérique et à ses risques
  - Des métiers et des hommes (Du directeur sécurité aux RSSI)
  - L'organisation de la sécurité en entreprise

2. Risques numériques (1h de e-learning, 1h30 de conférence)
- Définitions, référentiels
  - Gestion et traitements des risques
  - Méthodes
- Concepts
  - Impacts, biens primordiaux, menaces, scénarios, bien support, vulnérabilité...
  - Matrice de gravité
- Cadres normatifs
- ISO 27005
  - Intégration dans SMSI
  - AR dans les projets
- Des risques aux objectifs de sécurité
  - Risques résiduels
  - PDCA
- Vieille sécurité
  - CERT (vulnérabilités, menaces)
- ANSSI

3. Architectures & Technologies (2x1h en e-learning, 1h30 de conférence)
- De l'analyse de risques aux fonctions de sécurité (Filtrage, Accès, Cryptographie)
- Architecture et composants de système d'information
  - Front applications, middleware (BDD, serveurs messagerie), Endpoints (PC, Mobile, IOT ...), Réseau (Journaux: Traçabilité)
- Modèles de sécurité et technologies de sécurité protectrices
  - Château fort (FW, Proxy, anti DDoS), cloisonnement, accès admin dédié
  - Sondes de détection (IDS/IDP)
  - IAM , ZeroTrust, Bastion, VPN SSL, NAC
  - Multi Cloud – CASB
- Sécurité Endpoint
  - FW local, AntiVirus, EDS/EDR

4. Management de la sécurité (1h en e-learning, 1h30 de conférence)
- Contraintes légales et normatives
  - Contraintes d'état OIV, OSE, Défense ...
  - RGPD
- Construction de la Politique de sécurité du système d'information
  - PSG, comment passe-t-on de l'analyse de risques à une PSSI ?
- Système de Management de la Sécurité de l'Information (SMSI)
  - Introduction à ISO 27001, Historique et basiques, périmètre de certification,
  - Mesures ISO 27002
- Audit de conformité
  - Dashboard RSSI, indicateurs du niveau de sécurité
- Gestion de la continuité d'activité
  - Norme ISO 22301, définitions

5. La sécurité opérationnelle (3h en e-learning, 1h30 de conférence)
- Vulnerability Management
  - Facteurs HOT (Humain, Organisation, Techniques)
  - Audit, Pentest, CERT
  - Vulnerability Intelligence
- Threat Management
  - Techniques d'attaques
  - Log management
  - Détection et SIEM
  - Threat Intelligence
  - IOC, CTI
- Incident Management
  - CSIRT,
  - Process de gestion des incidents
  - Analyse Post-Mortem, forensique
  - Gestion de crise Cyber

6. La sécurité opérationnelle (1h en e-learning, 1h30 de conférence)
- Security By Design
  - Concepts et principes
  - Méthologies de MCS
- Règles techniques de sécurisation / durcissement
  - IAM, Systèmes d'exploitation, matériel, locaux, réseaux
- Organisation de la sécurité dans les projets
  - Missions des équipes, Ingénierie, Opération, Pilotage
- Sécurité des données sensibles
- Sécurité des produits
  - Conformité aux implémentations normatives, la confiance certifiée (CSPN, critères communs)

7. Le business de la cybersécurité (1h en e-learning, 1h30 de conférence)
- Les acteurs de référence
  - Editeurs
  - ESN
  - Opérateurs
  - Régulateurs
- Confiance, crédibilité
  - CyberRating
  - Prestataires Qualifiés par l'ANSSI
- La concurrence et le marché
  - Évolution du marché
  - Concurrence
- Les grands évènements
- FIC, ECW, Assises, ...
- CTF, Challenges
- Les associations professionnelles
- CESIN, CLUSIF, ...

Evaluation :

Après chaque module, évaluation par un test de connaissance.

NOUS CONTACTER

Cnam Bretagne
tél. : 02.57.52.05.48
brest@cnam-bretagne.fr

LE CNAM BRETAGNE VOTRE PARTENAIRE DE FORMATION EN BRETAGNE

DES FORMATIONS COURTES, CIBLÉES ET EFFICACES

CONSEILS PERSONNALISÉS POUR VOTRE ENTREPRISE

Nos conseillers dédiés sont à votre service pour vous guider dans toutes les étapes du processus de formation. De la prise en charge au financement, bénéficiez d'une écoute attentive et de conseils sur-mesure adaptés à votre entreprise.

DES FORMATIONS TOURNÉES VERS L'OPÉRATIONNALITÉ

Nos formations courtes sont rigoureusement conçues pour maximiser l'efficacité et l'impact sur votre activité. Des cas pratiques pertinents et des échanges d'expérience riches qui reflètent les défis réels de votre secteur sont proposés.

ACCESSIBILITÉ HANDICAP

Le Cnam Bretagne est engagé dans une démarche de progrès en matière d'accueil des personnes en situation de handicap. Notre référent se tient à votre disposition pour en échanger dès maintenant.