MAITRISE DU RISQUE

CYBERSECURITE

PROTEGER LES USAGES NUMERIQUES AU QUOTIDIEN

EFFICIOR
Conseil et Formation

INFORMATIONS ET TARIFS

Réf. :	26310
Type :	sur site (intra)
Public :	Tout public
Formateur :	Expert en cybersécurité certifié
Durée :	1 journée (7 heures)
Groupe :	jusqu'à 12 participants
Tarifs :	Sur site : 3 000 € net* par groupe Inter : 450 € net* par stagiaire
Modalités :	Evaluation des attentes du niveau en début de session Evaluation des acquis Questionnaire de satisfaction à l'issue de la formation Attestation de formation
Accessibilité :	Besoins spécifiques ou compensation handicap, nous contacter

* Exonération de TVA sur la formation.
Tarif net hors frais de déplacement du formateur.

COMPETENCES VISEES ET OBJECTIFS

Expliquer l'état actuel de la cybersécurité
Comprendre les principaux mécanismes
Identifier les risques d'atteinte à la sécurité des systèmes d'information et les bons usages

METHODES ET MOYENS PEDAGOGIQUES

Apports théoriques et contextuels
Etude de cas , analyse de jurisprudence
Retours d'expérience

PROGRAMME

ÉTAT ACTUEL DE LA CYBERSÉCURITÉ EN SANTÉ

Un contexte de plus en plus menaçant
Le fléau du Ransomware
Les impacts sur les établissements de santé

COMPRENDRE LES PRINCIPAUX MÉCANISMES DE CYBERATTAQUES ET LES IMPACTS

Principales définitions et vocabulaire
Les acteurs de la cyberattaque
Les besoins de sécurité de l'information
Les processus d'attaque

APPRÉHENDER LA RÉGLEMENTATION LIÉE

OIV et OSE

LES RESSOURCES HUMAINES ET LE SI

Le Rôle d'utilisateur du SI :

- Messagerie électronique
- Mots de passe et authentification
- Clés USB et périphériques amovibles
- Accès et partage de la donnée
- Nomadisme
- Sécurité du poste de travail
- Réseaux

Les 10 commandements de l'utilisateur
Le règlement général sur la protection des données
Les données de santé en établissement

LA GESTION DE L'INCIDENT DE SÉCURITÉ ET LES DISPOSITIFS DE RÉPONSES AUX ATTAQUES

L'incident de sécurité
Les premiers réflexes en cas d'attaque cyber
Dispositif d'escalade et gestion de la crise cyber
Les assistances externes
Dispositif de sauvegarde
Plan de continuité d'activité & Plan de reprise d'activité.

RETOUR D'EXPÉRIENCE ET PLAN D'ACTIONS CYBER

Construire son retour d'expérience et communiquer
Elaboration d'un plan d'action consécutif à une attaque cyber
Détails et mode opératoire des principaux scénarios d'attaques

LES BONNES PRATIQUES EN MATIÈRE DE CYBER SÉCURITÉ

- Identifier
- Protéger
- Détecter
- Répondre
- Restaurer