



# Renforcer la cybersécurité en ESMS



Présentiel



# Renforcer la cybersécurité en ESMS

Prix de la formation

**1200€**

Durée de la formation

**1 journée (7h)**

Format

**Présentiel ou visio**

Nombre de participants

**1 à 12**

Prérequis

**Aucuns**

Public concerné

**Tout professionnel intervenant en ESSMS**

Approche pédagogique

**Salle dédiée, supports projetés, exposés théoriques, études de cas, quizz, mise à disposition des supports et logiciel qualité interactif !**

[Nous contacter](#)

**/5**



Ce programme n'a pas encore été évalué

Cette formation vous donne **les bases** de la cybersécurité et du fonctionnement d'une infrastructure informatique.

Elle permet **d'identifier** les points sensibles, **repérer** les vulnérabilités et **mettre en œuvre des** solutions simples et concrètes pour sécuriser les usages numériques et réduire les risques cyber.

## Les objectifs de la formation

- ✓ **Comprendre** ce qu'est le cyber-risque et la cyber sécurité.
- ✓ **Apprendre** à identifier les vulnérabilités de son ESMS.
- ✓ **Connaître** ses responsabilités légales.
- ✓ **Découvrir** des solutions concrètes pour renforcer la sécurité informatique de son ESMS.

## Comment financer cette formation ?

Cette formation relève de la formation professionnelle continue. Elle peut être financée directement par votre établissement ou sur fonds propres.

# Programme de formation

**Module 1** • 1 heure 30

## Découvrir les bases et comprendre l'infrastructure informatique d'un ESMS

- Comprendre les rôles des administrateurs système, réseau et de sécurité.
- Analyse d'un schéma d'infrastructure informatique d'un ESMS.
- Repérer les points sensibles et Identifier ce qui doit être traité en priorité.

**Module 2** • 1 heure 30

## Comprendre d'où viennent les risques

- Identifier les profils à risque : personne malveillante, salarié maladroit, erreur humaine, perte/panne de matériel.
- Identifier le matériel fragile ou critique.
- Repérer les zones vulnérables de son système informatique.
- Découvrir des solutions simples ou avancées pour sécuriser son système informatique : bonnes pratiques, organisation, matériel, logiciels.

**Module 3** • 1 heure

## Vos responsabilités légales.

- Comprendre vos obligations envers la loi et la réglementation, vos collaborateurs et les personnes accompagnées.
- Comprendre les risques pour votre ESMS : perte de données, perte d'image, responsabilité légale et financière.

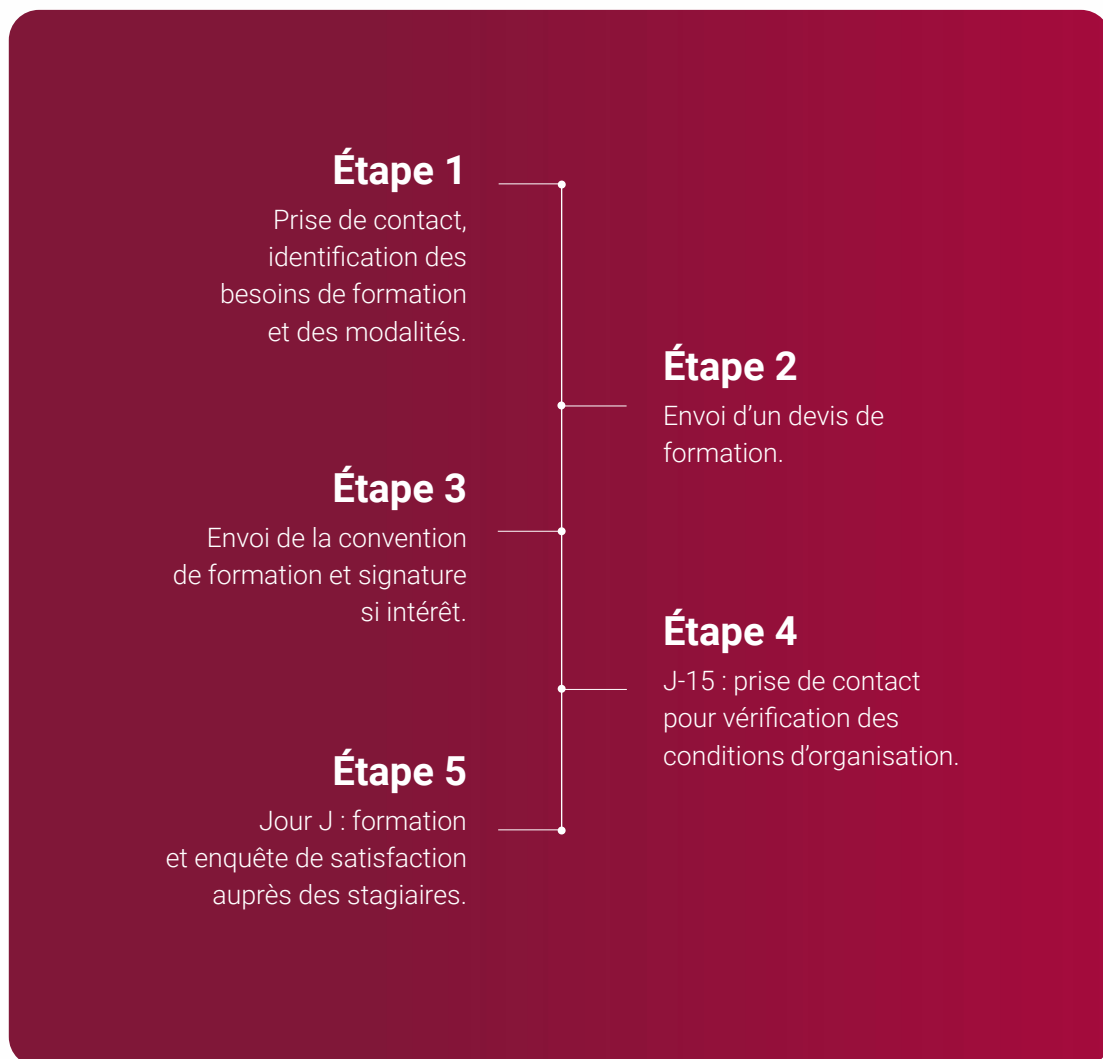
**Module 4** • 3 heures

## Etude de cas réel et mise en situation

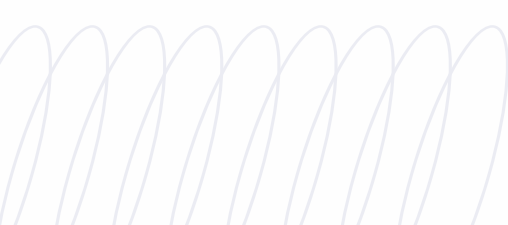
- Étude de cas réel d'incident de cybersécurité et de ses impacts sur l'entreprise.
- Les questions essentielles pour dialoguer efficacement avec le responsable du système informatique.
- Présentation concrète de la doctrine « **Sécuriser – Alerter – Sauvegarder – Réagir – Améliorer** » avec du matériel professionnel courant.



# Modalités d'accès



Les inscriptions sont possibles jusqu'à 15 jours avant le début de la session, sauf adaptation spécifique convenue. Le délai moyen entre la demande et l'entrée en formation est de 2 à 4 semaines.



## Modalités de suivi et d'exécution de la formation

- Entretien d'analyse des besoins en amont pour adapter la formation aux attentes du (des) bénéficiaire(s)
- Convocation envoyée en amont de la formation précisant les modalités de déroulement et de suivi de la formation
- Contrôle de la présence en formation via émargement digitalisé
- Enquête de satisfaction à chaud pour noter la formation par les apprenants.

## Modalités d'évaluation

- Évaluation de pré-formation en amont pour sonder les attentes et diagnostiquez le besoin avant la session
- Évaluation à froid pour mesurez l'impact professionnel de la formation pour entrer dans une démarche qualité quantitative
- Questionnaire pour les managers des apprenants afin d'évaluer la pertinence de la formation et son impact
- Chaque session donne lieu à une évaluation via un QCM à l'issue de la formation pour évaluer les compétences acquises et ainsi l'évaluation de l'atteinte des objectifs visés

## Équipe pédagogique

Nos formatrices et formateurs disposent d'une double expertise : une maîtrise approfondie de leur domaine d'intervention et une solide expérience de terrain dans le secteur concerné. Pour chaque projet de formation, le profil le plus pertinent est sélectionné en fonction du thème abordé et du type d'établissement accompagné.

## Contact



**Pierre BARA**

Directeur Général de Qualineo Performance

pierre@qualineo.io

0670205408

Référent pédagogique, handicap, administratif et technique

## Attestation de fin de formation

Une attestation de fin de formation et un certificat d'assiduité sont remis aux participants dès lors qu'ils ont suivi l'intégralité de la formation.

## Accessibilité aux personnes en situation de handicap (PSH)



L'ensemble de nos formations est accessible aux PSH. Une analyse est systématiquement réalisée en amont pour adapter les modalités pédagogiques et logistiques si nécessaire. Un référent handicap est mobilisable à tout moment.



**Qualineo**  
Performance



# Révélez vos équipes, montez en compétences

FORMATIONS • AUDITS • CONSEILS

[Nous contacter](#)