



**Les RH et la cybersécurité**  
Appréhender le rôle des RH en termes de cybersécurité – Ref. 2407

<b>Formation Inter ou intra entreprise</b>	
<b>Taux de satisfaction :</b>	N/A
<b>Durée</b>	<b>7 heures</b>
<b>Certification</b>	Aucune
<b>Prix</b>	Inter entreprise : 1.100 euros H.T Intra entreprise : Nous consulter

Cette formation est destinée aux RH et leurs équipes avec pour objectif d’appréhender les enjeux de la cybersécurité et le rôle attendu des RH dans la prévention et la gestion de la crise cybersécurité.

<b>Pré-requis</b>	<ul style="list-style-type: none"> <li>• Aucun</li> </ul>
<b>Public concerné</b>	<ul style="list-style-type: none"> <li>• Directeur et responsable des Ressources Humaines</li> <li>• Chargé d’études RH</li> <li>• Manager des ressources humaines</li> <li>• Cadres RH</li> <li>• RRH</li> </ul>
<b>Nombre de stagiaires</b>	<ul style="list-style-type: none"> <li>• Minimum 4 à 12 personnes</li> </ul>
<b>Délai d’accès au public</b>	<ul style="list-style-type: none"> <li>• 2 semaines à compter de la demande de formation</li> <li>• Pour les formations ‘sur-mesure’, deux entretiens préliminaires sont proposés pour définir ensemble la session de formation souhaitée</li> </ul>
<b>Objectifs pédagogiques</b> <b>A la fin du cours l’apprenant sera en mesure de :</b>	<ul style="list-style-type: none"> <li>• S’appropriier les enjeux cybersécurité d’un point de vue RH</li> <li>• Intégrer les enjeux de cybersécurité dans les plans d’actions, la gestion et la politique RH de l’entreprise</li> <li>• Connaître le rôle attendu des RH en termes de cybersécurité</li> </ul>
<b>Compétences visées</b>	<ul style="list-style-type: none"> <li>• Etre à même de contribuer à développer une culture cybersécurité au sein de son organisation</li> <li>• Mieux comprendre les attentes des RSSI / CISO</li> <li>• Pouvoir contribuer à préparer et gérer une gestion de crise cyber</li> </ul>



	<ul style="list-style-type: none"> <li>Pouvoir intégrer le plan de développement des compétences cyber pour les collaborateurs</li> </ul>
<b>Méthode d'évaluation</b>	<ul style="list-style-type: none"> <li>Phase d'évaluation : questionnaire sous la forme d'un QCM. Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant la formation.</li> </ul>
<b>Certificat de stage</b>	<ul style="list-style-type: none"> <li>Attestation de fin de stage</li> </ul>
<b>Tests de certification</b>	<ul style="list-style-type: none"> <li>Aucun</li> </ul>
<b>Références bibliographiques &amp; sitographiques utilisés pour ce module de formation</b>	<ul style="list-style-type: none"> <li><a href="https://www.alliancy.fr/rh-acteur-strategie-cybersecurite">https://www.alliancy.fr/rh-acteur-strategie-cybersecurite</a></li> <li><a href="https://www.alliancy.fr/competences-cyber-sensibilisation">https://www.alliancy.fr/competences-cyber-sensibilisation</a></li> </ul>
<b>Méthodes pédagogiques</b>	<ul style="list-style-type: none"> <li>En français ou en anglais</li> <li>Remise d'une documentation pédagogique numérique à la fin du stage</li> <li>La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience</li> <li>Les échanges seront encouragés autour de retours d'expériences, témoignages des participants.</li> </ul>
<b>Débouché et suite du parcours</b>	<ul style="list-style-type: none"> <li>Compétence transversale sur la gestion des compétences cyber au sein de son organisation pour l'ensemble des collaborateurs.</li> <li>Gestion du recrutement, de la formation et du développement du personnel.</li> <li>Approfondissement des connaissances acquises sur les métiers et les compétences cyber</li> </ul>
<b>Lieu</b>	<ul style="list-style-type: none"> <li>Dans nos locaux, sur site ou à distance</li> </ul>
<b>Nom et prénom de l'intervenant</b>	<ul style="list-style-type: none"> <li>Anne Doré ou autre formateur expert en cybersécurité</li> </ul>
<b>Éléments de biographie de l'intervenant</b>	<ul style="list-style-type: none"> <li>Anne Doré - Anne possède une solide expérience dans le conseil pour CSC Peat Marwick puis chez IBM, un des leaders mondiaux de la cyber sécurité.</li> <li>Elle a accompagné de nombreux dirigeants dans la mise en œuvre de projets stratégiques intégrant de nouvelles technologies (cloud, AI, big data) et la transformation des organisations.</li> </ul>



	<ul style="list-style-type: none"><li>• Sa devise ‘La cybersécurité est l’affaire de tous, notamment celle des dirigeants et des comités de direction’</li><li>• Autre formateur : à préciser selon le calendrier et les modalités d’intervention</li></ul>
<b>Modalités d’accès</b>	<ul style="list-style-type: none"><li>• Pour vous inscrire vous pouvez nous contacter à l’adresse suivante : <a href="mailto:contact@adhel.fr">contact@adhel.fr</a></li><li>• Ou remplir le questionnaire ci-joint</li><li>• Nous nous engageons à vous répondre dans les 48H</li></ul>

### Contenu de la formation

#### Les fondamentaux de la cybersécurité

- Comprendre les enjeux de la cybersécurité
- S’approprier les principaux types de risque

#### Les RH acteurs de la gestion de crise cyber

- Anticiper et préparer la gestion de crise
- Être acteur de la gestion de crise
- Gérer la situation post crise

#### Les compétences et la culture cyber

- Développer les compétences de l’ensemble des collaborateurs
- Intégrer la cybersécurité dans la culture de son organisation

#### La cybersécurité, la diversité et l’inclusion

- Les enjeux RH en termes de cybersécurité
- Faire de la cybersécurité une opportunité de diversité

#### Conclusion : les RH partenaires du CISO et RSSI

### FIN DU DOCUMENT

#### CONTACT :

Mél: [contact@adhel.fr](mailto:contact@adhel.fr)  
Tél. +33 6 60 26 27 48  
<https://adhel.fr>

ADHEL – 63 rue Nationale - 92100 Boulogne Billancourt  
Siret : 88274050900014 – NDA : 11922660392  
Organisme de formation Qualiopi au titre des actions de formation continue



Tous droits réservés