ODESIA

DATA · IA · CYBERSECURITE

CATALOGUE DE FORMATION

Cybersécurité

Stratégie · Outils de productivité · Formation technique

Toutes les formations sont offertes en présentiel ou en ligne.

INTRODUCTION

Un catalogue pour renforcer la cybersécurité de l'organisation

La cybersécurité n'est plus l'affaire des seuls spécialistes : elle engage les dirigeants, chaque employé et les équipes techniques. ODESIA Intelligence propose un catalogue de formations structuré en trois catégories, pour accompagner chaque profil de l'organisation, du comité de direction aux équipes techniques.

Vue d'ensemble

	CATÉGORIE	PUBLIC PRINCIPAL	DURÉES
01	**Stratégie** 9 formations	Dirigeants, cadres, responsables de la sécurité et de la conformité	**1 à 3 jours**
02	**Outils de productivité** 9 formations	Tous les employés	**0,5 à 1 jours**
03	**Formation technique** 10 formations	Professionnels TI et sécurité	**2 à 5 jours**

Modalités communes

- Présentiel ou en ligne : toutes les formations peuvent être suivies dans l'un ou l'autre format, au choix de l'organisation.
- Durée : exprimée en jours de formation. Les durées indiquées sont celles du format standard de chaque formation.
- Parcours intégrés : chaque catégorie propose un parcours qui regroupe plusieurs formations pour une montée en compétences progressive.
- Contenus adaptables : les formations peuvent être ajustées au secteur, au niveau et aux outils de l'organisation. **Contactez-nous pour une proposition sur mesure.**

CATÉGORIE 01

Stratégie

Gouverner la cybersécurité et décider en connaissance de cause.

Ces formations s'adressent aux dirigeants, aux cadres, aux responsables de la sécurité, de la conformité et des risques. Elles aident à définir l'orientation, à arbitrer les investissements et à encadrer la gestion des risques, sans compétence technique préalable.

Formations proposées

FORMATION	OBJECTIF	DURÉE
Cybersécurité pour dirigeants et conseils d'administration	Comprendre les enjeux, les responsabilités et les questions à poser pour exercer une supervision éclairée de la cybersécurité.	**1 jour**
Élaboration de la stratégie de cybersécurité et feuille de route	Définir une vision, des priorités et un plan de mise en œuvre réaliste, alignés sur les risques et les objectifs de l'organisation.	**2 jours**
Gouvernance, gestion des risques et conformité	Structurer les rôles, les politiques et le processus d'évaluation des risques, et s'appuyer sur des référentiels reconnus.	**2 jours**
Loi 25, protection des renseignements personnels et incidents de confidentialité	Comprendre les obligations applicables et savoir comment les intégrer à la gestion des risques et des incidents.	**1 jour**
Gestion de crise cyber : exercice de simulation	Mettre à l'épreuve la prise de décision de la direction lors d'un incident majeur, à partir d'un scénario réaliste.	**1 jour**
Continuité des activités et résilience	Identifier les processus critiques, définir les objectifs de reprise et planifier le rétablissement après un incident.	**1 jour**
Gestion des risques liés aux tiers et aux fournisseurs	Évaluer, encadrer contractuellement et suivre la posture de sécurité des fournisseurs et des partenaires.	**1 jour**
Cybersécurité et intelligence artificielle : risques et gouvernance	Cerner les risques propres à l'IA et définir les règles d'utilisation, de contrôle et de protection des données.	**1 jour**
Programme exécutif « Stratégie cybersécurité » (parcours intégré)	Parcours combinant gouvernance, gestion des risques, conformité et gestion de crise, aboutissant à une feuille de route adaptée à l'organisation.	**3 jours**

Offerte en présentiel ou en ligne.

CATÉGORIE 02

Outils de productivité

Travailler efficacement, en toute sécurité.

Ces formations courtes et pratiques s'adressent à l'ensemble des employés. Elles développent les bons réflexes pour utiliser les outils du quotidien (courriel, infonuagique, appareils mobiles, outils d'IA) de façon sécuritaire, sans freiner la productivité.

Formations proposées

FORMATION	OBJECTIF	DURÉE
Sensibilisation à la cybersécurité pour tous les employés	Comprendre les principales menaces et le rôle de chacun dans la protection de l'organisation.	**0,5 jour**
Hameçonnage et ingénierie sociale	Reconnaître les tentatives de fraude par courriel, texto ou téléphone, et savoir comment réagir.	**0,5 jour**
Mots de passe, authentification multifacteur et gestionnaires de mots de passe	Adopter des pratiques d'authentification solides et utiliser les outils qui les simplifient.	**0,5 jour**
Sécuriser le télétravail et les appareils mobiles	Protéger ses appareils, ses connexions et ses données en dehors du bureau.	**0,5 jour**
Utilisation sécuritaire des outils collaboratifs et de l'infonuagique	Partager des fichiers, gérer les accès et collaborer en ligne sans exposer d'informations sensibles.	**0,5 jour**
Protection des données sensibles au quotidien	Savoir classer, conserver, partager et détruire les données selon leur niveau de sensibilité et les politiques internes.	**0,5 jour**
Utilisation sécuritaire des outils d'IA générative	Tirer parti de l'IA sans divulguer de données confidentielles et en vérifiant les résultats obtenus.	**0,5 jour**
Réflexes en cas d'incident : détecter et signaler	Savoir reconnaître un incident, quoi faire dans les premières minutes et à qui le signaler.	**0,5 jour**
Parcours « Employé cyber-vigilant » (parcours intégré)	Parcours regroupant les fondamentaux, l'hameçonnage, l'authentification, le travail à distance et les bons réflexes en cas d'incident.	**1 jour**

Offerte en présentiel ou en ligne.

CATÉGORIE 03

Formation technique

Développer l'expertise des équipes TI et sécurité.

Ces formations s'adressent aux professionnels des TI et de la sécurité : administrateurs, analystes, développeurs, ingénieurs, architectes. Les prérequis sont précisés lors de l'inscription, selon le niveau de chaque formation.

Formations proposées

FORMATION	OBJECTIF	DURÉE
Fondamentaux de la cybersécurité	Acquérir les bases : menaces, vulnérabilités, contrôles de sécurité et principes de défense en profondeur.	**3 jours**
Sécurité des réseaux et des infrastructures	Concevoir, segmenter et protéger les réseaux, et déployer les contrôles de sécurité périmétriques et internes.	**3 jours**
Sécurité de l'infonuagique	Sécuriser les environnements infonuagiques : configuration, gestion des accès, protection des données et responsabilités partagées.	**3 jours**
Gestion des identités et des accès	Mettre en place l'authentification, les droits d'accès et la gestion des comptes à privilèges selon le moindre privilège.	**2 jours**
Durcissement des systèmes et des terminaux	Réduire la surface d'attaque des serveurs et des postes de travail grâce à des configurations sécurisées et au suivi des correctifs.	**2 jours**
Sécurité des applications et développement sécurisé	Intégrer la sécurité tout au long du cycle de développement et corriger les failles applicatives courantes.	**3 jours**
Tests d'intrusion et évaluation des vulnérabilités	Identifier et exploiter des vulnérabilités dans un cadre autorisé, puis documenter les constats et les correctifs.	**5 jours**
Détection et surveillance : opérations de sécurité	Collecter et analyser les journaux, détecter les comportements suspects et trier les alertes dans un centre d'opérations de sécurité.	**5 jours**
Réponse aux incidents et investigation numérique	Contenir un incident, préserver les preuves, mener l'analyse technique et rétablir les systèmes.	**5 jours**
Sécurité des systèmes d'IA	Identifier et réduire les risques propres aux systèmes d'IA : fuite de données, manipulation des modèles, usages malveillants.	**3 jours**

Offerte en présentiel ou en ligne.

RÉCAPITULATIF

Toutes les formations en un coup d'œil

01 STRATÉGIE		
Cybersécurité pour dirigeants et conseils d'administration	Présentiel / En ligne	1 jour
Élaboration de la stratégie de cybersécurité et feuille de route	Présentiel / En ligne	2 jours
Gouvernance, gestion des risques et conformité	Présentiel / En ligne	2 jours
Loi 25, protection des renseignements personnels et incidents de confidentialité	Présentiel / En ligne	1 jour
Gestion de crise cyber : exercice de simulation	Présentiel / En ligne	1 jour
Continuité des activités et résilience	Présentiel / En ligne	1 jour
Gestion des risques liés aux tiers et aux fournisseurs	Présentiel / En ligne	1 jour
Cybersécurité et intelligence artificielle : risques et gouvernance	Présentiel / En ligne	1 jour
Programme exécutif « Stratégie cybersécurité » (parcours intégré)	Présentiel / En ligne	3 jours
02 OUTILS DE PRODUCTIVITÉ		
Sensibilisation à la cybersécurité pour tous les employés	Présentiel / En ligne	0,5 jour
Hameçonnage et ingénierie sociale	Présentiel / En ligne	0,5 jour
Mots de passe, authentification multifacteur et gestionnaires de mots de passe	Présentiel / En ligne	0,5 jour
Sécuriser le télétravail et les appareils mobiles	Présentiel / En ligne	0,5 jour
Utilisation sécuritaire des outils collaboratifs et de l'infonuagique	Présentiel / En ligne	0,5 jour
Protection des données sensibles au quotidien	Présentiel / En ligne	0,5 jour
Utilisation sécuritaire des outils d'IA générative	Présentiel / En ligne	0,5 jour
Réflexes en cas d'incident : détecter et signaler	Présentiel / En ligne	0,5 jour
Parcours « Employé cyber-vigilant » (parcours intégré)	Présentiel / En ligne	1 jour
03 FORMATION TECHNIQUE		
Fondamentaux de la cybersécurité	Présentiel / En ligne	3 jours
Sécurité des réseaux et des infrastructures	Présentiel / En ligne	3 jours
Sécurité de l'infonuagique	Présentiel / En ligne	3 jours
Gestion des identités et des accès	Présentiel / En ligne	2 jours
Durcissement des systèmes et des terminaux	Présentiel / En ligne	2 jours
Sécurité des applications et développement sécurisé	Présentiel / En ligne	3 jours
Tests d'intrusion et évaluation des vulnérabilités	Présentiel / En ligne	5 jours
Détection et surveillance : opérations de sécurité	Présentiel / En ligne	5 jours
Réponse aux incidents et investigation numérique	Présentiel / En ligne	5 jours
Sécurité des systèmes d'IA	Présentiel / En ligne	3 jours

CONTACT

Pour planifier une formation, composer un parcours ou obtenir une proposition sur mesure, envoyez-nous un courriel à l'adresse suivante : info@odesia.com