

Mis à jour le 22/08/2025

S'inscrire

Formation Les enjeux de la cybersécurité dans son organisation - pour les dirigeants

3 jours (21 heures)

Présentation

Notre formation sur les enjeux de la cybersécurité dans son organisation s'adresse spécifiquement aux dirigeants, cadres et responsables informatiques afin de leur donner une vision claire, stratégique et pragmatique des risques cyber.

Vous découvrirez comment s'approprier les enjeux stratégiques de la sécurité numérique dans son organisation.

La formation couvre aussi bien la gestion des risques que les aspects réglementaires et inclut des ateliers pratiques basés sur des scénarios réels.

À l'issue de ce parcours, vous serez en mesure d'identifier les menaces stratégiques pour votre organisation, de définir un plan d'action concret et de renforcer la culture cyber au sein de vos équipes.

Comme toutes nos formations, celle-ci est basée sur les dernières évolutions réglementaires et technologiques en matière de cybersécurité et privilégie une approche pratique et opérationnelle.

Objectifs

- Comprendre les enjeux stratégiques de la cybersécurité dans une organisation
- Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture
- Connaître le cadre réglementaire et les obligations légales
- Favoriser une culture cyber dans l'entreprise

Public visé

- Dirigeants d'entreprises
- Cadre d'entreprise
- Responsable informatique

Pré-requis

- Aucun prérequis

Programme de notre formation Les enjeux de la cybersécurité dans son organisation

[Jour 1 - Matin]

Panorama des menaces et impacts business

- Évolution des menaces : ransomware, supply chain, fraude, ingénierie sociale
- Identifier ses actifs critiques et sa surface d'attaque
- Impacts économiques, juridiques et réputationnels : coûts directs/indirects
- Exemples d'attaques ciblées vs opportunistes (PME / grand compte)
- Lecture d'un scénario de risque orienté métier
- Atelier pratique : Analyse rapide d'un incident type et estimation d'impact.

Gouvernance, rôles et responsabilités

- Aligner la stratégie cyber avec la stratégie d'entreprise
- Rôles du COMEX, DSI, RSSI, métiers et prestataires
- Politiques, chartes et comité de sécurité
- Culture sécurité : sensibilisation et exemplarité du management
- Budget, arbitrages et priorisation

[Jour 1 - Après-midi]

Réglementations et standards (NIS2, RGPD, ISO 27001, NIST CSF)

- Périmètre et obligations clés de NIS2 pour les secteurs concernés
- Articulation RGPD / sécurité : registre, DPO, violation de données
- Démarche ISO/IEC 27001 (ISMS) et contrôles
- Cadre NIST CSF 2.0 : organiser et mesurer la posture
- Feuille de route de conformité pragmatique

Gestion des risques et priorisation des investissements

- Identifier, évaluer et traiter les risques (cartographie & heatmap)
- Fraude à la fausse facture : Business Email Compromise (BEC)
- Contrôles essentiels : IAM, patching, sauvegardes, EDR, MFA
- Approche Zero Trust et segmentation
- Assurance cyber : garanties, exclusions, exigences
- Atelier pratique : Prioriser un plan d'actions à budget contraint.

[Jour 2 - Matin]

Gestion de crise et continuité d'activité (PCA/PRA)

- Chaîne d'alerte et responsabilisation des acteurs : instaurer des réflexes communs face à l'incident
- Scénarios vécus : rançongiciel, fuite de données, déni de service, avec rôle de chacun dans la réponse
- Plan de continuité et de reprise (RTO/RPO) comme outil collectif et non seulement technique
- Communication de crise : transparence et cohérence pour préserver la confiance (autorités, partenaires, clients, médias)
- Partenaires stratégiques (assureurs, prestataires IR/DFIR) : développer une relation de confiance avant la crise
- Atelier pratique : Simulation de crise cyber. Mise en situation d'un COMEX confronté à une attaque et la posture de leadership adoptée, avec un focus sur la prise de décision, la communication et le pilotage collectif.

Développer une culture partagée de la cybersécurité

- Exemplarité et engagement du top management comme levier de diffusion culturelle
- Sensibilisation différenciée : COMEX, managers, collaborateurs, partenaires
- Communication interne régulière : campagnes, rituels, journées cybersécurité, storytelling d'incidents
- Intégration dans les pratiques métiers : « security by design » et indicateurs culturels dans les projets
- Valorisation et reconnaissance : encourager les bonnes pratiques et la remontée d'incidents
- Atelier pratique : Co-crédation d'une charte managériale cyber. Définir en groupes 5 engagements concrets que les dirigeants porteront auprès de leurs équipes.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de

sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.