



SF FORMATIONS | SAS, société par actions simplifiée au capital social de 1 000,00 € |  
N° SIRET 892.767.617.00012 | N° de TVA FR70892767617 ·  
Certification Qualiopi n° ATA I35 2024 | Enregistré sous le numéro 768 200 998 82  
Cet enregistrement ne vaut pas agrément de l'Etat.

## PROGRAMME DE FORMATION

### *Les enjeux de la cybersécurité dans son organisation – pour les dirigeants (1,5 jour)*

#### **Public cible**

Dirigeants d'entreprises, cadres d'entreprise, responsables informatiques.

#### **Prérequis**

- Cette formation ne nécessite pas de prérequis.

#### **Objectifs finaux**

À l'issue de la formation, le stagiaire sera capable de s'approprier les enjeux et clés stratégiques de la sécurité numérique dans son organisation :

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

#### **Méthodologie pédagogique**

Formation construite selon le cycle d'apprentissage expérientiel de Kolb :

1. Expérience concrète : immersion dans des cas concrets vécus par des dirigeants face à des cyberincidents.
  2. Observation réfléchie : analyse des réactions, impacts et décisions prises.
  3. Conceptualisation : apports sur les enjeux stratégiques, la gouvernance, la réglementation et la culture cyber.
  4. Expérimentation active : ateliers collaboratifs pour élaborer un plan stratégique cybersécurité.
- Modalités : classe virtuelle interactive, études de cas réels, échanges entre pairs, outils collaboratifs (Miro, Proton), restitution collective.



SF FORMATIONS | SAS, société par actions simplifiée au capital social de 1 000,00 € |  
N° SIRET 892.767.617.00012 | N° de TVA FR70892767617 ·  
Certification Qualiopi n° ATA I35 2024 | Enregistré sous le numéro 768 200 998 82  
Cet enregistrement ne vaut pas agrément de l'Etat.

## Programme détaillé (10.5h)

### Panorama de la cybersécurité pour dirigeants (2h)

- Impacts sur la gouvernance
- Tendances et menaces actuelles

Modalité : Présentation interactive + échanges entre participants

Evaluation par Quiz interactif

### Cybersécurité et gouvernance d'entreprise (2h)

- Rôle du dirigeant
- Adaptation des processus

Modalité : Atelier collaboratif sur Miro

Evaluation par Restitution orale

### Cadre réglementaire et obligations légales (2h)

- Principales lois et normes
- Impacts sur l'organisation

Modalité : Étude de cas pratique

Evaluation par QCM de validation

### Développer une culture cyber dans l'entreprise (2h)

- Sensibilisation et communication
- Implication des équipes

Modalité : Atelier de construction d'un plan de sensibilisation

Évaluation du plan produit

### Synthèse et plan d'action stratégique (2h)

- Élaboration d'une feuille de route
- Engagements des participants

Modalité : Travail en groupe sur un plan stratégique



SF FORMATIONS | SAS, société par actions simplifiée au capital social de 1 000,00 € |  
N° SIRET 892.767.617.00012 | N° de TVA FR70892767617 ·  
Certification Qualiopi n° ATA I35 2024 | Enregistré sous le numéro 768 200 998 82  
Cet enregistrement ne vaut pas agrément de l'Etat.

## Scénario fil rouge

Contexte : 'TechLeaders Group', entreprise multisite, fait face à une augmentation des attaques ciblant son conseil d'administration et ses équipes de direction. Les participants, en tant que dirigeants, élaborent une stratégie globale de cybersécurité intégrée à la gouvernance de l'entreprise.

### Modalités d'évaluation et livrables

Évaluations formatives : quiz, études de cas, restitution d'ateliers.

Évaluation sommative : présentation d'un plan stratégique cybersécurité.

Livrables : plan stratégique cybersécurité, plan de sensibilisation, fiche synthèse réglementaire.

### Critères d'évaluation (grille)

| Critère                     | Description  |
|-----------------------------|--|
| Compréhension des enjeux    | Capacité à identifier les enjeux stratégiques de la cybersécurité. |
| Pertinence des solutions    | Adéquation des propositions avec la réalité organisationnelle.     |
| Intégration réglementaire   | Prise en compte correcte des obligations légales.                  |
| Qualité du plan stratégique | Structure, clarté et pertinence du plan présenté.                  |
| Implication                 | Participation active aux échanges et ateliers.                     |