# Développer des systèmes et infrastructures cyber-résilients

**Durée :** **3** jours **Prix :** 2 850 € HT

## Contexte

Comment expliquer l'augmentation constante des attaques réussies au moment où les organisations déploiement des efforts énormes (technologiques, financiers, humains, etc.) pour se prémunir des cyberattaques ?

Le risque « **zéro** » n'existe pas. Et c'est là tout le problème des solutions actuelles. En outre, l'hétérogénéité des systèmes, infrastructures et applications rend très difficile la mise en oeuvre de la défense en profondeur. Dès lors, les organisations dans leur immense majorité concentrent leurs efforts sur la seule protection de leur réseau local. Le réseau local étant lui-même très vulnérable à l'ingénierie sociale.

Les nouvelles tendances de la sécurité des systèmes et infrastructures s'orientent vers la « **cyber-résilience** ». Elle est définie comme « la capacité d'anticiper, de résister, de récupérer et de s'adapter à des conditions défavorables, des contraintes, des attaques ou des compromissions sur des systèmes qui utilisent ou sont activés par des cyber-ressources ». Les systèmes dotés de cette propriété se caractérisent par des mesures de sécurité « intégrées » en tant que partie fondamentale de l'architecture et de la conception. De plus, ces systèmes peuvent résister aux cyberattaques, aux pannes et aux défaillances et peuvent continuer à fonctionner même dans un état dégradé ou affaibli, en exerçant des fonctions essentielles à la mission de l'organisation et en garantissant que les autres aspects de la fiabilité (en particulier, la sûreté et la sécurité) sont conservés.

L'INSTITUT DENOF propose ce cours aux organisations dans le but de les former à l'ingénierie de la cyber-résilience.

## Objectifs

- S'approprier les concepts et principes fondamentaux de la cyber-résilience.
- Connaître la différence entre cybersécurité et cyber-résilience.
- Découvrir les pratiques de la cyber-résilience.
- Mettre en oeuvre la cyber-résilience : cycle de vie.

## Public visé

Top Management, Managers, Responsables de la sécurité des systèmes, Gestionnaires et Exploitants des Assets, Cadres et toute personne intéressée par la stratégie de cybersécurité.

## Prérequis

Aucun.

## Modalités pratiques

### Méthodologie pédagogique

Exposé, échanges d’expérience, études de cas.

### Méthodologie d'évaluation

Le stagiaire reçoit en amont de la formation un questionnaire permettant de mesurer les compétences, profil et attentes du stagiaire. Tout au long de la formation, les stagiaires sont évalués au moyen de différentes méthodes (quizz, ateliers, exercices et/ou de travaux pratiques, etc.) permettant de vérifier l'atteinte des objectifs. Un questionnaire d'évaluation à chaud est soumis à chaque stagiaire en fin de formation pour s'assurer de l'adéquation des acquis de la formation avec les attentes du stagiaire. Une attestation de réalisation de la formation est remise au stagiaire.

## Programme

### Module 1 : Concepts et principes fondamentaux de la cyber-résilience

- Buts de la cyber-résilience
- Objectifs de la cyber-résilience
- Techniques et approches de la cyber-résilience
- Principes de conception de la cyber-résilience
- Relation entre les concepts de la cyber-résilience
- La cyber-résilience dans le cycle de vie d'un système
- Gestion des risques et cyber-résilience
- La défense en profondeur

### Module 2 : Sélection et hiérarchisation des actions de cyber-résilience

- Réalisation des buts et objectifs
- Stratégie de gestion des risques cyber
- Type de système
- Conflits et synergies de la cyber-résilience
- Autres disciplines et investissements existants
- Architectures
- Effets sur les adversaires, les menaces et les risques
- Maturité et adoption de la cyber-résilience

### Module 3 : Pratiques et processus analytiques

- Compréhension du contexte
- Établir les critères de base de la cyber-résilience
- Analyser le système
- Définir et analyser des solutions alternatives
- Développer des recommandations

### Module 4 : Cyber-résilience dans les processus du cycle de vie du système

- Analyse des missions de l'organisation
- Définition des besoins et des exigences des parties prenantes
- Définition des exigences du système
- Définition de l'architecture
- Définition de la conception
- Analyse du système
- Mise en œuvre
- Intégration
- Vérification
- Transition
- Validation

- Mise en service
- Maintenance.