Cybersécurité et intelligence économique

Des vols de données au blocage des systèmes informatiques, les cyberattaques peuvent avoir des conséquences désastreuses. Venez vous former aux principes de la souveraineté et de la sécurité numériques de vos organisations à travers l'étude de cas concrets.

Crédit image | ©Institut national du service public (INSP)

Cette formation est organisée en partenariat avec l'Institut des hautes études de défense nationale (IHEDN).

La formation en un coup d'œil

- **Date de la formation** : Mercredi 5 novembre 2025
- **Durée** : 2 jour(s)
- **Lieu** : École Militaire, 75007 Paris
- **Prix** : 700 €
- **Langue** : Français
- **Format** : Présentiel

Public cible

- Cadres supérieurs de la fonction publique
- Cadres supérieurs du secteur privé

Pré-requis

La formation ne nécessite aucun prérequis et repose sur une démarche volontaire.

Une forte motivation pour les enjeux de souveraineté numérique et de défense nationale au sens large.

Compétences visées

- → Développer une vision stratégique
- → Innover
- → Piloter la performance
- → S'adapter
- → Transformer

Objectifs de la formation

- → Acquérir une vision d'ensemble des enjeux de la souveraineté numérique.
- → Mieux appréhender les actions de l'État en matière de protection numérique.
- → Comprendre les risques résultant des mauvaises pratiques numériques.
- → Identifier les points de contacts institutionnels et les procédures à suivre en cas d'attaques cyber.
- → Étudier des cas concrets de vulnérabilité numérique.

Profil des intervenants

Experts issus des institutions de l'État en charge des questions de cybersécurité comme l'ANSSI, le COMGENDCYBER ou le GIP ACYMA.

Programme

Jour 1

Introduction aux enjeux macro de la cybersécurité et de la souveraineté numérique

Défis, enjeux et menaces de la cybersécurité

- → Exploration des défis actuels de la cybersécurité, y compris les cyberattaques et les cybermenaces
- → Analyse des enjeux liés à la protection des données, à la confidentialité et à l'intégrité des systèmes informatiques
- → Identification des différentes formes de menaces cyber et des méthodes d'attaque courantes

Les enjeux juridiques du cyber

→ Étude des cadres juridiques nationaux et internationaux régissant la cybersécurité et la souveraineté numérique
→ Analyse des lois et réglementations liées à la protection des données personnelles et à la sécurité des systèmes d'information
→ Discussion sur les défis juridiques liés à la lutte contre la cybercriminalité et à la gestion des incidents cybernétiques

La protection institutionnelle contre les menaces cyber

→ Évaluation des meilleures pratiques et des politiques de cybersécurité au niveau institutionnel
→ Discussion sur la mise en place de mesures de protection et de prévention des cyberattaques dans les organisations
→ Exploration des outils et des technologies utilisés pour renforcer la résilience des infrastructures informatiques contre les menaces cyber

Jour 2

Ateliers pratiques et introduction à l'Open Source INTelligence (OSINT)

Ateliers pratiques et introduction à l'OSINT

→ Atelier pratique « Hack me if you can »
→ Atelier pratique de l'OSINT

Pédagogie

Modalités d'évaluation

Présence sur l'intégralité du programme, compréhension de la méthode et des possibilités de mise en pratique à son poste. Evaluation sous forme d'une enquête de satisfaction et évaluation des acquis à travers les mises en situation durant la formation.

Modalités pédagogiques

La formation articule des apports thématiques, théoriques, méthodologiques à des mises en situation. Les mises en situation font l'objet de débriefing collectifs et d'apports complémentaires de méthode.

Moyens pédagogiques

Supports pédagogiques de l'intervenant.

Modalités d'inscription

Formation participative, groupe de 30 à 40 personnes

Indicateurs

Nos auditeurs et auditrices plébiscitent nos formations : 4,6/5 de satisfaction et 95 % de recommandation en 2024 !