INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

PRÉSENTATION DE LA FORMATION

Cycle spécialisé

Sécurité des usages numériques

2017-2018

SISSE Commissaire et Service de l'Information Stratégique et de la Sécurité Économiques

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

CLÔTURE DES INSCRIPTIONS :
27 OCTOBRE 2017

Cycle spécialisé – **2017-2018**

Sécurité des usages numériques

OBJECTIFS DE LA FORMATION

L'information est désormais au cœur des actifs immatériels de l'entreprise et constitue un élément clé de sa performance. L'évolution de l'Internet a par ailleurs conféré aux systèmes d'information une dimension incontournable du développement de l'économie. La sécurité numérique représente donc un enjeu majeur pour la pérennité et la compétitivité des entreprises.

Le Cycle spécialisé « Sécurité des usages numériques » est supervisé par le Département Intelligence et Sécurité économiques de l'INHESJ en partenariat avec le Club informatique des grandes entreprises françaises (CIGREF).

L'INHESJ est un établissement public national à caractère administratif placé sous la tutelle du Premier ministre. L'INHESJ intervient dans les domaines de la formation, des études, de la recherche, de la veille et de l'analyse stratégique en matière de sécurité intérieure, sanitaire, environnementale et économique ainsi que dans ceux intéressant la justice et les questions juridiques.

Le CIGREF, association de Grandes Entreprises, a quant à lui pour vocation de « *Promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise* ». Il mène également un programme international de recherche sur ces thématiques, au travers de la Fondation CIGREF (sous égide de la Fondation Sophia Antipolis).

Ce Cycle se fixe pour objectifs de délivrer les savoir-faire visant l'identification, l'évaluation et la maîtrise de l'ensemble des risques et des malveillances à tous ceux qui veulent mieux comprendre les enjeux de la Sécurité Numérique au sein des entreprises.

Institut national des hautes études de la sécurité et de la justice
École militaire – Case n°39
1 place Joffre – 75700 Paris 07 SP

Contact : département Intelligence et Sécurité économiques

Tél : +33 (0)1 76 64 89 93
Fax : +33 (0)1 76 64 89 31
Courriel : securite-economique@inhesj.fr

Site internet : www.inhesj.fr

Télécharger le **Dossier de candidature**

Télécharger la **Convention de formation**

Cycle spécialisé – **2017-2018**

Sécurité des usages numériques

PUBLICS DE RÉFÉRENCE

Il s'adresse aux personnes issues du secteur privé et de la sphère institutionnelle :

- dirigeants, managers métiers, responsables fonctions ;
- managers sécurité/sûreté, gestionnaires de risques, crises ;
- responsables de la sécurité des systèmes d'information (RSSI) ;
- consultants en sécurité informatique ;
- directeurs des systèmes d'information (DSI) ou responsables du service informatique ;
- chefs de projet informatique en charge du projet sécurisation ;

Les stagiaires du Cycle spécialisé « Sécurité des usages numériques » sont recrutés sur dossier.

ORGANISATION PÉDAGOGIQUE DE LA SESSION

L'ensemble du C ycle est fondé sur les enseignements opérationnels et le partage d'expériences. Les cours magistraux se combinent à des présentations concrètes émanant de praticiens expérimentés.

Le panel des intervenants est très large : il est composé de représentants d'administrations centrales (ANSSI - Agence nationale de la sécurité des systèmes d'information, BEFTI – Préfecture de Police de Paris, DGSI - Direction générale de la sécurité intérieure, DRSD - Direction du Renseignement et de la Sécurité de la Défense, Etat-Major des Armées, Ministère de l'Europe et des Affaires étrangères, Ministère de la Justice, OCLCTIC - Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, Pôle Judiciaire de la Gendarmerie Nationale...), de cadres dirigeants d'entreprises (DSI, RSSI, Directeur des Risques, Directeur juridique, Directeur Sûreté...) qui témoignent de leurs pratiques du terrain en France et à l'étranger, ainsi que des experts spécialisés (Autorités administratives indépendantes telle la CNIL – Commission Nationale Informatique & Libertés, des avocats, cabinets d'audit, groupes d'intérêt, universitaires...) qui complètent par leurs approches respectives les différentes dimensions de la sécurité numérique.

Un exercice de gestion de crise en situation complète cette formation.

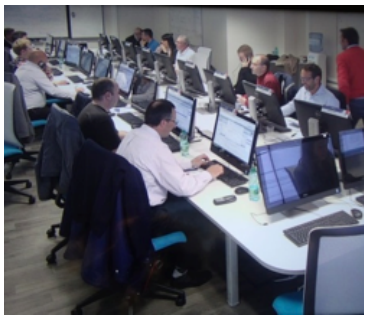
Télécharger le **Dossier de candidature**

Télécharger la **Convention de formation**

• La documentation

Une documentation abondante, variée et constamment mise à jour est remise aux auditeurs plusieurs semaines avant chaque module afin de leur permettre de préparer les rencontres dans les meilleures conditions. Ces supports fournissent les éléments d'information en français et en anglais pour rendre possibles des échanges fructueux avec l'intervenant et une compréhension des enjeux liés aux sujets traités lors des différents modules.

• Mise en situation de gestion de crise



Un exercice de mise en situation de gestion de crise a été intégré au Cycle. L'exercice est conduit à partir de scenarii « entreprise », en temps et en situation réels. Les auditeurs sont répartis au sein d'une cellule de crise, en responsabilité d'un poste spécifique, nécessitant des réactions, des analyses et des décisions de chacun. L'animation est organisée de manière à placer les membres de la cellule en situation de stress contrôlé.

Les auditeurs sont ainsi plongés au cœur d'une cyber attaque en entreprise, sur le plateau de l'Institut.

• Les visites en institutions et/ou entreprises

Outre cette mise en situation, les auditeurs sont confrontés à la sécurité des usages numériques en institutions et/ou entreprises lors des visites organisées par le département chez ses partenaires.

• Travail de groupe

Plusieurs petits groupes d'auditeurs se voient attribuer un thème à fort enjeu, fondé sur l'actualité récente de la cyber sécurité. Chaque groupe de travail se réunit tout au long de l'année pour proposer des réflexions et des préconisations dans le cadre d'un rapport écrit.

En fin de cycle, ce rapport fait l'objet d'une restitution collective notamment devant de grands témoins, experts du sujet.

DEROULEMENT DU CYCLE

L'ensemble des enseignements en session plénière comporte un volume de 96 heures (6 heures x 16 jours) réparties sur 16 jours, à raison de 2 jours par mois sur une durée de 8 mois, auxquelles s'ajoutent le temps d'élaboration et de production du rapport final qui sera présenté en fin de cycle par chacun des groupes de travail.

Les cours magistraux ont lieu au siège de l'Institut à l'Ecole militaire à Paris. Toutefois, des visites organisées par le département chez des partenaires (institutionnels et/ou entreprises) pourront occasionner des déplacements en France.

Télécharger le **Dossier de candidature**

Télécharger la **Convention de formation**

Cycle spécialisé – **2017-2018**

Sécurité des usages numériques

Programme previsionnel

Du 20 au 21 novembre 2017 - Module 1

Quelle gouvernance de l'Internet ?

- Comment fonctionne Internet ?
- Qui gouverne dans le Cyberespace ? Etats, entreprises, hacktivistes, internautes...
- Quelles sont les forces en présence ?
- Quelle cyberdiplomatie pour la France ?
- Quelle géopolitique à l'ère numérique ?

Du 18 au 19 décembre 2017 - Module 2

Les missions de police sur le Net

- Quel ordre public sur la Toile ?
- Comment travaillent les services de police et de gendarmerie sur le Net ?
- Comment travailler avec eux ?
- Comment porter plainte après une cyberattaque ?
- Que risque-t-on en se connectant ?

Du 22 au 23 janvier 2018 - Module 3

Quel(s) droit(s) à l'heure d'internet ?

- Quelles sont les spécificités du droit sur Internet ?
- Comment le faire appliquer ?
- Quelles sont les règles ?
- Quelles précautions prendre ?
- Comment prendre en compte les évolutions techniques ?
- Comment faire exécuter des décisions de justice à l'étranger ?
- Quelles sont les procédures à respecter ?
- Quels sont les tribunaux et les régimes juridiques compétents ?

Du 5 au 6 février 2018 - Module 4

Quelle défense à l'heure de la cyberguerre ?

- La cyberguerre est-elle une réalité ?
- Si oui que recouvre-t-elle ?
- Quelles implications pour les citoyens et les entreprises ?
- Quelles sont les nouvelles règles d'affrontement quand les cibles et les assaillants sont des Etats, des entreprises ou des personnes isolées ?
- Qu'est-ce qu'une arme dans le monde numérique ?

Du 5 au 6 mars 2018 - Module 5

Attaques informationnelles : quand l'info devient une arme

- Atteintes à la réputation, campagne de dénigrement, vol d'informations : quelles sont les protections envisageables, les moyens de veille et les contre-mesures à déployer en cas d'attaque ?
- Quel rôle pour les réseaux sociaux ?
- Quels stratégie et entrainements doivent être adoptés par les entreprises, voire les individus ?
- Un exercice très réaliste met en situation les auditeurs afin de les confronter à la réalité d'une crise cyber.

Du 3 au 4 avril 2018 - Module 6

Cybersécurité : Nouveaux enjeux & nouveaux acteurs

- Big Data, Blockain, Intelligence artificielle, logiciels malveillants, monnaies virtuelles, objets connectés, start-up émergentes, vers informatiques ... les parties prenantes et les technologies disponibles sont en constante évolution. Comment les connaître et les intégrer dans la transformation numérique des entreprises et des administrations ?

Du 2 au 3 mai 2018 - Module 7

Vie privée, technologies et cybersécurité

- Les données personnelles et la vie privée sont au cœur des questions de sécurité numérique. Quelles sont les concessions envisageables pour les citoyens ?
- Quelles sont les stratégies des GAFAM (Google, Amazon, Facebook, Apple, Microsoft...) et quel est leur impact sur la sécurité numérique des personnes et des entreprises ?
- Comment fonctionnent les outils d'attaques ?
- Quelles sont les technologies en devenir dans le domaine de la cybersécurité ?
- Quelle place pour l'anonymat sur le Net ? Qu'est-ce qu'un droit à l'oubli effectif ?

Du 4 au 5 juin - Module 8

Soutenance des rapports et clôture du Cycle

- Cet ultime module permet d'enrichir par des interventions complémentaires les sujets abordés au cours de l'année. C'est également lors de cette session qu'interviennent les soutenances devant un jury d'experts des rapports rédigés par les groupes de travail. Afin de valider l'obtention des diplômes.

Télécharger le **Dossier de candidature**

Télécharger la **Convention de formation**

VALIDATION DU CYCLE

Les stagiaires admis à suivre ce Cycle spécialisé ont une obligation d'assiduité aux séminaires et aux déplacements, conformément aux dispositions de l'engagement d'assiduité en annexe de la convention de formation.

Cette assiduité aux cours ainsi que la remise d'un rapport, dont le sujet est arrêté par le Département Intelligence et Sécurité économiques en début de cycle, valident cette formation, par la délivrance d'un certificat de spécialisation.

DROITS D'INSCRIPTION

Les droits d'inscription au **Cycle spécialisé « Sécurité des usages numériques »** sont fixés à **5 000 euros.**

Les droits d'inscription sont exigibles dans leur intégralité avant l'ouverture du Cycle.

Les frais afférents à l'hébergement, à la restauration et au transport sont à la charge du stagiaire ou de son employeur, excepté pour ce qui est prévu par le programme dans le cadre des déplacements.

FORMATION PROFESSIONNELLE

L'Institut national des hautes études de la sécurité et de la justice est habilité à percevoir des fonds au titre de la formation professionnelle. Une convention de formation spécifique et une facture sont alors établies.

CLÔTURE DES INSCRIPTIONS :
27 OCTOBRE 2017

Télécharger le **Dossier de candidature**

Télécharger la **Convention de formation**