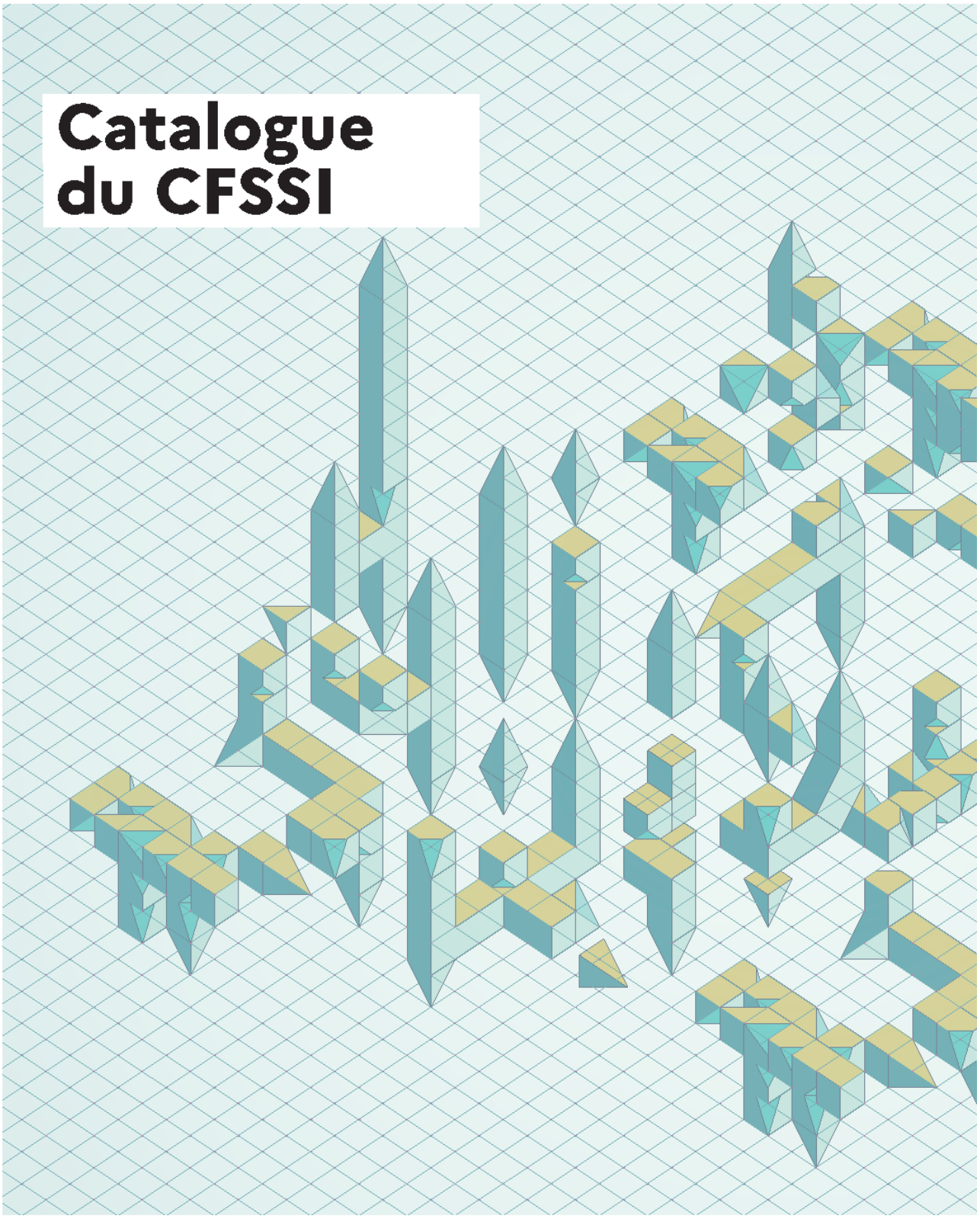
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Catalogue du CFSSI



CATALOGUE DES STAGES 2023 DU CFSSI

Le CFSSI est le centre de formation à la sécurité des systèmes d'information de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Le CFSSI propose, chaque année, une trentaine de stages courts couvrant de nombreux domaines de la sécurité des systèmes d'information. D'une durée d'une journée à plusieurs semaines et offrant une large palette de niveaux de technicité, ces stages sont accessibles aux seuls agents de l'administration française : Etat, Collectivités territoriales et fonction publique hospitalière, ainsi qu'aux membres des OIV. Les stages courts du CFSSI sont assurés en présentiel dans les locaux du Campus Cyber de la Défense, Tour Eria*(*)*.

(*) En cas de formation délivrée à distance, un guide de connexion à la plateforme de visioconférence est adressé au stagiaire ; aucune des formations en distanciel n'est enregistrée.

Il est rappelé que :

* les demandes de stages sont adressées par l'organisme d'emploi dont relève le stagiaire et impérativement validées par une autorité reconnue par le CFSSI ;
* les stages sont gratuits mais les repas ainsi que l'hébergement demeurent à la charge du stagiaire ou de son organisme d'appartenance ;
* au début de chaque formation, le stagiaire doit se munir d'une pièce d'identité et de sa convocation afin de pouvoir accéder aux salles de formation. Pour certains stages, un certificat d'habilitation de niveau « secret » sera demandé ;
* chaque formation fait l'objet d'une attestation adressée au stagiaire dans un délai d'un mois à l'issue de sa formation ainsi que du support pédagogique du formateur. Les stages courts du CFSSI ne sont en revanche ni certifiants ni diplômants. Chaque stagiaire est destinataire, à l'issue de la formation, d'un questionnaire d'évaluation de formation, à retourner au CFSSI ;
* le calendrier des formations est prévisionnel et il est susceptible d'évoluer en fonction des contraintes opérationnelles de l'ANSSI.

CFSSI - Campus Cyber - 5 rue Bellini - 92800 Puteaux -
Mél : cfssi@cfssi.gouv.fr

Catalogue 2023							
n° stage	Stages	Janvier	Février	Mars	Avril	Mai	Juin
1.	Panorama de la sécurité des systèmes d'information		9 Fév.		6 Avril		1 Juin
2a.	Premier pas en Tempest					11 Mai	
2.	Sécurité électromagnétique et Tempest						12-16 Juin
3.	Investigaton numérique						26-30 Juin
4.	La Méthode EBIOS		13-14 Fév.	13-14 Mars		22-23 Mai	
5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	30-31 Janv.			3-4 Avril		19-20 Juin
5b.	Utiliser l'outil Informatique de manière sécurisée (Pratique)		1-3 Fév.				21-23 Juin
6.	Certificats électroniques		20-22 Fév.				13-15 Juin
7a.	Internet et la sécurité	9-13 Janv.		6-10 Mars			12-16 Juin
8a.	Principes et organisation des audits en sécurité des systèmes d'information	5-6 Janv.			17-18 Avril	9-10 Mai	
8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes)		13-17 Fév.			22- 26 Mai	26-30 Juin
9.	Sécurité des applications Web			20-24 Mars			
10.	Cryptographie			7-10 Mars 20-24 Mars	3-7 Avril 17-21 Avril		
11a.	Sécurité des réseaux sans fils	17-20 Janv.				9-12 Mai	
12.	Homologation Sécurité			27-28 Mars			
14.	Incidents de sécurité			7-10 Mars	17-20 Avril		
16.	Intégrer la sécurité numérique dans les projets SI de l'Etat				20-21 Avril		
17a.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects théoriques et réglementa	23-27 Janv.					5-9 Juin
17b.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects techniques		13-17 Fév.				19-23 Juin
18.	Enjeux stratégiques de la Cybersécurité				24-26 Avril		
19.	Sécurité des systèmes industriels		1-3 Fév.		11-13 Avril		
20.	Cloud Computing enjeux de sécurité				11-12 Avril		
21.	Administration sécurié Windows			20-24 Mars			
22.	Incubateur de CSIRT						
23.	Sécurité physique et logique des composants						5-9 Juin
24.	Analyse de vulnérabilités logiciels					22-26 Mai	
25.	Sécurité des systèmes embarqués			27-29 Mars			
26.	Sécurité des architectures virtualisées	10-12 Janv.				15-17 Mai	
27.	Sécurité firmware et chaîne de démarrage			15-17 Mars			
29.	Gestion de crise (volet opérationnel, stratégique, communication)						26-28 Juin
30.	Analyste SOC				3-7 Avril		

Catalogue 2023							
n° stage	Stages	Juillet	Août	Septembre	Octobre	Novembre	Décembre
1.	Panorama de la sécurité des systèmes d'information				19 Oct.	27 Nov.	
2a.	Premier pas en Tempest				20 Oct.		
2.	Sécurité électromagnétique et Tempest					13-17 Nov.	
3.	Investigaton numérique	3-7 Juil.				6-10 Nov. 20-24 Nov.	
4.	La Méthode EBIOS			5-6 Sept.		6-7 Nov.	4-5 déc.
5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)			25-26 Sept.		6-7 Nov.	
5b.	Utiliser l'outil Informatique de manière sécurisée (Pratique)			27-29 Sept.		8-10 Nov.	
6.	Certificats électroniques				3-5 Oct.		
7a.	Internet et la sécurité			11-15 Sept.	9-13 Oct.		4-8 Déc.
8a.	Principes et organisation des audits en sécurité des systèmes d'information			18-19 Sept.			13-14 Déc.
8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes)				23-27 Oct.	20-24 Nov.	
9.	Sécurité des applications Web					27 Nov. - 1 Déc.	
10.	Cryptographie						
11a.	Sécurité des réseaux sans fils			18-21 Sept.			
12.	Homologation Sécurité	3-4 Juil.			23-24 Oct.		
14.	Incidents de sécurité			11-14 Sept.	9-12 Oct.		
16.	Intégrer la sécurité numérique dans les projets SI de l'Etat				9-10 Oct.		
17a.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects théoriques et réglementaires			18-22 Sept.		20-24 Nov.	
17b.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects techniques				2-6 Oct.		4-8 Déc.
18.	Enjeux stratégiques de la Cybersécurité				16-18 Oct.		
19.	Sécurité des systèmes industriels			27-29 Sept.		20-22 Nov.	
20.	Cloud Computing enjeux de sécurité			27-28 Sept.			
21.	Administration sécurié Windows						4-8 Déc.
22.	Incubateur de CSIRT				16-25 Oct.		
23.	Sécurité physique et logique des composants						
24.	Analyse de vulnérabilités logiciels						11-15 Déc.
25.	Sécurité des systèmes embarqués						
26.	Sécurité des architectures virtualisées					14-16 Nov.	11-13 Déc.
27.	Sécurité firmware et chaîne de démarrage					13-15 Nov.	
29.	Gestion de crise (volet opérationnel, stratégique, communication)					27-29 Nov.	
30.	Analyste SOC	3-7 Juil.					

CALENDRIER des formations 2023

Peut évoluer en fonction des contraintes opérationnelles de l'ANSSI

	Janvier 2023	
Stage 5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	30-31 Janv.
Stage 7a.	Internet et la Sécurité	09-13 Janv.
Stage 8a.	Principes et organisation des audits en sécurité des systèmes d'information	05-06 Janv.
Stage 11a.	Sécurité des réseaux sans fils	17-20 Janv.
Stage 17a.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects théoriques et réglementaires	23-27 Janv.
Stage 26.	Sécurité des architectures virtualisées	10-12 Janv.
	Février 2023	
Stage 1.	Panorama de la sécurité des systèmes d'information	09 Fév.
Stage 5b.	Utiliser l'outil Informatique de manière sécurisée (TP)	01-03 Fév.
Stage 4.	La Méthode EBIOS Risk Manager	13-14 Fév.
Stage 6.	Certificats Electroniques (TP)	20-22 Fév.
Stage 8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes) (TP)	13-17 Fév.
Stage 17b.	Responsable de la Sécurité des systèmes d'information (RSSI) (Aspects techniques)	13-17 Fév.
Stage 19.	Sécurité des systèmes industriels	01-03 Fév.
	Mars 2023	
Stage 4.	La Méthode EBIOS Risk Manager	13-14 Mars
Stage 7a.	Internet et la Sécurité	6-10 Mars
Stage 9.	Sécurité des applications Web	20-24 Mars
Stage 10.	Cryptographie	07-10 Mars 20-24 Mars
Stage 12.	Homologation Sécurité	27-28 Mars
Stage 14.	Incidents de Sécurité (TP)	07-10 Mars
Stage 21.	Administration sécurité Windows (TP)	20-24 Mars
Stage 25.	Sécurité des systèmes embarqués	27-29 Mars
Stage 27.	Sécurité firmware et chaîne de démarrage	15-17 Mars
	Avril 2023	
Stage 1.	Panorama de la sécurité des systèmes d'information	06 Avril.
Stage 5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	03-04 Avril

CALENDRIER des formations 2023

Peut évoluer en fonction des contraintes opérationnelles de l'ANSSI

	Avril 2023	
Stage 8a.	Principes et organisation des audits en sécurité des systèmes d'information	17-18 Avril
Stage 10.	Cryptographie	03-07 Avril 17-21 Avril
Stage 14.	Incidents de Sécurité (TP)	17-20 Avril
Stage 16.	Intégrer la sécurité numérique dans les projets SI de l'Etat	20-21 Avril
Stage 18.	Enjeux Stratégiques de la Cybersécurité	24-26 Avril
Stage 19.	Sécurité des systèmes industriels	11-13 Avril
Stage 20.	Cloud Computing enjeux de sécurité	11-12 Avril
Stage 30.	Analyste SOC (TP)	03-07 Avril
	Mai 2023	
Stage 2a.	Premiers pas en Tempest	11 Mai
Stage 4.	La Méthode EBIOS Risk Manager	22-23 Mai
Stage 8a.	Principes et organisation des audits en sécurité des systèmes d'information	09-10 Mai
Stage 8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes) (TP)	22- 26 Mai
Stage 11a.	Sécurité des réseaux sans fils	09-12 Mai
Stage 24.	Analyse de vulnérabilités logiciels	22-26 Mai
Stage 26.	Sécurité des architectures virtualisées	15-17 Mai
	Juin 2023	
Stage 1.	Panorama de la sécurité des systèmes d'information	01 Juin.
Stage 2	Sécurité électromagnétique et Tempest	12-16 Juin
Stage 3.	Investigation numérique	26-30 Juin
Stage 5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	19-20 Juin
Stage 5b.	Utiliser l'outil Informatique de manière sécurisée (TP)	21-23 Juin
Stage 6.	Certificats Electroniques (TP)	13-15 Juin
Stage 7a.	Internet et la Sécurité	12-16 Juin
Stage 8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes) (TP)	26-30 Juin

CALENDRIER des formations 2023

Peut évoluer en fonction des contraintes opérationnelles de l'ANSSI

	Juin 2023	
Stage 17a.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects théoriques et réglementaires	05-09 Juin
Stage 17b.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects techniques	19-23 Juin
Stage 23.	Sécurité physique et logique des composants (TP)	05-09 Juin
Stage 29.	Gestion de crise (Volet opérationnel, Stratégique, Communication)	26-28 Juin
	Juillet 2023	
Stage 3.	Investigation numérique	03-07 Juil.
Stage 12.	Homologation Sécurité	03-04 Juil.
Stage 30.	Analyste SOC (TP)	03-07 Juil.
	Septembre 2023	
Stage 4.	La Méthode EBIOS Risk Manager	05-06 Sept.
Stage 5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	25-26 Sept.
Stage 5b.	Utiliser l'outil Informatique de manière sécurisée (TP)	27-29 Sept.
Stage 7a.	Internet et la Sécurité	11-15 Sept.
Stage 8a.	Principes et organisation des audits en sécurité des systèmes d'information	18-19 Sept.
Stage 11a.	Sécurité des réseaux sans fils	18-21 Sept.
Stage 14.	Incidents de Sécurité (TP)	11-14 Sept.
Stage 17a.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects théoriques et réglementaires	18-22 Sept.
Stage 19.	Sécurité des systèmes industriels	27-29 Sept.
Stage 20.	Cloud Computing enjeux de sécurité	27-28 Sept.
	Octobre 2023	
Stage 1.	Panorama de la sécurité des systèmes d'information	19 Oct.
Stage 2a.	Premiers pas en Tempest	20 Oct.
Stage 6.	Certificats électroniques (TP)	03-05 Oct.
Stage 7a.	Internet et la Sécurité	09-13 Oct.
Stage 8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes) (TP)	23-27 Oct.
Stage 12.	Homologation Sécurité	23-24 Oct.
Stage 14.	Incidents de Sécurité (TP)	09-12 Oct.
Stage 16.	Intégrer la sécurité numérique dans les projets SI de l'Etat	09-10 Oct.
Stage 17b.	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects techniques	02-06 Oct.

CALENDRIER des formations 2023

Peut évoluer en fonction des contraintes opérationnelles de l'ANSSI

	Octobre 2023	
Stage 18.	Enjeux stratégiques de la Cybersécurité	16-18 Oct.
Stage 22.	Incubateur de CSIRT	16-25 Oct.
	Novembre 2023	
Stage 1.	Panorama de la sécurité des systèmes d'information	27 Nov.
Stage 2.	Sécurité électromagnétique et Tempest	13-17 Nov.
Stage 3.	Investigation numérique	06-10 Nov. 20-24 Nov.
Stage 4.	La Méthode EBIOS Risk Manager	06-07 Nov.
Stage 5a.	Utiliser l'outil Informatique de manière sécurisée (Théorie)	06-07 Nov.
Stage 5b.	Utiliser l'outil Informatique de manière sécurisée (TP)	08-10 Nov.
Stage 8b.	Principes et organisation des audits en sécurité des systèmes d'information (Aspect systèmes) (TP)	20-24 Nov.
Stage 9.	Sécurité des applications Web	27 Nov. - 01 Déc.
Stage 17a.	Responsable de la sécurité des systèmes d'information (RSSI) - (Aspects théoriques et réglementaires)	20-24 Nov.
Stage 19.	Sécurité des systèmes industriels	20-22 Nov.
Stage 26.	Sécurité des architectures virtualisées	14-16 Nov.
Stage 27.	Sécurité firmware et chaîne de démarrage	13-15 Nov.
Stage 29.	Gestion de crise (volet opérationnel, stratégique, communication)	27-29 Nov.
	Décembre 2023	
Stage 4.	La Méthode EBIOS Risk Manager	04-05 déc.
Stage 7a.	Internet et la sécurité	04-08 déc.
Stage 8a.	Principes et organisation des audits en sécurité des systèmes d'information	13-14 déc.
Stage 17b.	Responsable de la sécurité des systèmes d'information (RSSI) (Aspects techniques)	04-08 déc.
Stage 21.	Administration sécurisée Windows (TP)	04-08 déc.
Stage 24.	Analyse de vulnérabilités logiciels	11-15 déc.
Stage 26.	Sécurité des architectures virtualisées	11-13 Déc.

SOMMAIRE des fiches descriptives par stage

Panorama de la sécurité des systèmes d'information

Réf. 1 | **Durée. 1 jour** | **Présentiel ou Distanciel**

Objectifs

Proposer un bref tour d'horizon des différents domaines de la sécurité des systèmes d'information et fournir quelques clés de compréhension

Programme

* Principaux risques ;
* Notions SSI ;
* Organisation nationale de la SSI ;
* Obligations juridiques ;
* Description succincte des composantes techniques de la SSI.

Niveau

Initiation

Public

Décideurs conscients des enjeux et soucieux de s'informer. Autorités en charge de la SSI, nouvellement affectées.

Prérequis

Aucun prérequis

Thématique

Découverte de la cybersécurité

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Premiers pas en TEMPEST

Réf. 2a	Durée. 1 jour	Présentiel

Présentation

Présentation des menaces apportées par les ondes électromagnétiques en confidentialité (TEMPEST), mais aussi en intégrité et en disponibilité (AGREMI).

Un aperçu de l'organisation des réglementations française et internationales est présenté.

Objectifs

Sensibiliser les participants à la menace liée aux ondes électromagnétiques sur les systèmes d'information classifiés ou sensibles dans leur environnement quotidien.

Programme

* Présentation des menaces TEMPEST et AGREMI ;
* Veille sources publiques ;
* Réglementation TEMPEST nationale et internationale ;
* Les cas particuliers hors réglementation ;
* Les règles d'installation - Démarche de sécurisation ;
* Le zonage TEMPEST.

Niveau

Initiation

Public

Toute personne amenée à traiter des informations classifiées.

! Prérequis

Les apprenants doivent être habilités au niveau SECRET ou supérieur et doivent être munis de leur certificat d'habilitation dès le premier jour du stage. Dans le cas contraire, ils ne seront pas acceptés à participer au stage.

Thématique

Organisation des réglementations TEMPEST françaises et internationales

Moyens de protection contre la menace TEMPEST

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité électromagnétique (TEMPEST)

Réf. 2	Durée. 5 jours	Présentiel

Présentation

Ce stage présente les menaces apportées par les ondes électromagnétiques en confidentialité (TEMPEST), mais aussi en intégrité et en disponibilité (AGREMI). Un panorama des réglementations françaises et internationales est présenté. Des ateliers pratiques permettent de mettre en application et d'illustrer les notions abordées.

Objectifs

* Comprendre les menaces que font peser les ondes électromagnétiques sur la sécurité des systèmes d'information ;
* Être apte à identifier les menaces pour pouvoir déterminer les mesures à prendre pour préserver la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Programme

Jour 1
* Présentation des menaces TEMPEST et AGREMI
* Veille sources publiques
* Rappels de physique
* Aspects juridiques de la protection contre les SPC

Jour 2
* Réglementation TEMPEST nationale et internationale
* Le zonage TEMPEST
* Les règles d'installation - 1ère partie
* L'évaluation normative des équipements

Jour 3
* AGREMI et Cyber sécurité
* Air-Gap
* Les règles d'installation - 2ème partie

Jour 4
* Cage de FARADAY Théorie

Jour 5
* Mise en situation : étude de cas en groupe
* TEMPEST appliqué aux systèmes

Niveau

Perfectionnement

Public

Personnels appelés à assurer la protection des systèmes d'information contre les émissions de signaux compromettants.

Prérequis

Les apprenants doivent être habilités au niveau SECRET ou supérieur et doivent être munis de leur certificat d'habilitation dès le premier jour du stage. Dans le cas contraire, ils ne seront pas acceptés à participer au stage.

Thématique

Réglementation TEMPEST française et internationale,

Présentation des agressions électromagnétiques intentionnelles (AGREMI).

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Investigation numérique

Réf. 3 | **Durée. 10 jours** | **Présentiel ou Distanciel**

Objectifs

Approfondir les connaissances en investigation numérique par la compréhension du fonctionnement des systèmes d'exploitation et l'exploitation de traces numériques.

Programme

* Acquisition et exploitation des empreintes mémoire ;
* Analyse et reconstruction de volumes complexes (LVM, RAID) ;
* Journalisation, collecte et traces spécifiques à l'environnement macOS ;
* Journalisation, collecte et traces spécifiques à l'environnement Windows ;
* Journalisation, collecte et traces spécifiques à l'environnement Linux ;
* Journalisation et collecte des traces réseau ;
* Chaque module comprend un cours, ainsi que des cas pratiques.

Niveau

Expert

Public

Personnes disposants déjà de compétences en matière d'investigation numérique et souhaitant approfondir ces connaissances.

Ingénieurs en investigation numérique (experts judiciaires, N-TECH, ICC).

! Prérequis

Connaissances en investigation numérique.

Thématique

Approfondissement des connaissances en investigation numérique

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

La Méthode EBIOS Risk Manager

Réf. 4 | **Durée. 2 jours** | **Présentiel ou Distanciel**

Présentation

Pour assurer ses missions, l'organisation relative au management des risques numériques doit développer trois valeurs fondamentales : la connaissance, l'agilité et l'engagement. EBIOS Risk Manager offre une compréhension et une responsabilité partagées des risques numériques entre décideurs et les acteurs opérationnels pour y parvenir. L'objectif est de permettre aux dirigeants d'appréhender correctement ces risques, au même titre que d'autres de nature stratégique, financière, juridique, d'image, de ressources humaines, etc. La méthode EBIOS, méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques.

Objectifs

Être capable d'utiliser la méthode EBIOS Risk Manager pour réaliser ou piloter une étude des risques.

Programme

* Concepts de la gestion des risques et grands principes de la méthode EBIOS Risk Manager ;
* Identification du socle de sécurité ;
* Description des événements redoutés, identification des impacts et de la gravité ;
* Prise en compte de la notion d'écosystème ;
* Élaboration des scénarios stratégiques et opérationnels ;
* Traitement des risques et mesures de sécurité ;
* Amélioration continue de la sécurité et mise en place du cadre de suivi des risques.

Niveau

Perfectionnement

Public

Personnes en charge de mener une analyse de risques cybersécurité et de conseiller une autorité dans sa gestion des risques cyber (RSSI, FSSI, CSN, chef de projet, conseiller, etc.).

Prérequis

Pratique de la SSI

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Utiliser l'outil informatique de manière sécurisée (Théorie)

Réf. 5a | **Durée. 2 jours** | **Présentiel ou Distanciel**

Présentation

Informer sur les risques associés à Internet et sur les moyens d'y faire face. Des recommandations pratiques pour utiliser l'outil informatique de manière sécurisée y sont présentées.

Objectifs

Comprendre les méthodes utilisées par les attaquants pour compromettre un poste de travail depuis Internet.

Identifier les moyens pour s'en protéger.

Programme

* **Sécurité de la messagerie électronique** : le courrier électronique (POP et SMTP), pièces jointes, identification, confidentialité ;
* **Sécurité Web** : modes de communication, outils, services et sécurité, le web, la navigation, SSL/TLS, cookies, codes mobiles, les navigateurs ;
* **Sécurité du poste de travail** : introduction aux principales notions de sécurité des systèmes d'information : risques, cryptographie, certificats et racines de confiance ;
* **Antivirus** : les principales menaces (malwares, vulnérabilités) et moyens de protection, outils de sécurité : contre quelles menaces nous protègent-ils ? L'exemple des antivirus.

Niveau

Initiation

Public

Personnes souhaitant découvrir macroscopiquement les aspects techniques et organisationnels de la cybersécurité (RSSI, correspondant informatique et SSI, formateurs, et autres personnels pouvant jouer le rôle de relais auprès des utilisateurs).

! Prérequis

Aucun prérequis

Thématique

Sécurité de la messagerie électronique

Sécurité Web

Sécurité du poste de travail

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Utiliser l'outil informatique de manière sécurisée

Réf. 5b | **Durée. 3 jours** | **En présentiel (TP)**

Présentation

Présenter les techniques de sécurisation des postes de travail à travers l'exploration des fonctions indispensables à un travail partagé.

Sensibiliser aux menaces principales et donner un certain nombre de réflexes notamment dans la configuration et l'utilisation quotidienne des postes de travail.

Objectifs

Sensibiliser les stagiaires aux risques inhérents à l'outil informatique et aux services numériques et leur présenter les points d'attention lors de leur utilisation (configuration de leur poste de travail, utilisation de mots de passe robustes, configurations recommandées pour l'usage des services numériques).

Programme

Jour 1 : Le poste de travail
Sécurisation de la phase de démarrage, chiffrement de disque, critères de choix du système d'exploitation, bonnes pratiques d'utilisation des comptes privilégiés, configurations avancées des droits, recommandations sur les mots de passe, mises à jour du poste, utilisation d'un parefeu, d'un anti-virus, d'un effaceur sécurisé.

Jour 2 : Introduction à la cryptographie
Historique, différence entre chiffrement symétrique et asymétrique, objectifs du la cryptographie asymétrique, présentation de PGP et du chiffrement avec certificats.

Jour 3 : Sécurité sur Internet.
Présentation rapide historique, les différences entre Internet visible, profond et sombre, le principe d'encapsulation du trafic réseau, la mécanique de résolution de nom, ses risques et ses traces, l'accès à un site web, ses risques et ses traces, le fonctionnement d'un navigateur Internet et les bonnes pratiques de configuration.

Jour 4 : Messagerie électronique
Les menaces qu'elle peut véhiculer, le fonctionnement de l'envoi et la réception d'un courriel, la sécurisation des communications ou du contenu, les risques spécifiques des webmails et la configuration du client de messagerie.

Jour 5 : Risques de sécurité liés au nomadisme (en environnement Microsoft) et aux mesures de sécurité qui permettent de les limiter, qu'ils s'agisse des risques qui pèsent sur le poste de travail Windows lui-même ou sur le SI face à un poste potentiellement compromis.
Des exercices pratiques reposent sur l'utilisation d'outils de chiffrement, de restriction logicielle, de VPN, de parefeu logiciel, de réutilisation de secrets d'authentification, etc.

Niveau

Initiation

Public

Personnes souhaitant découvrir les bonnes pratiques en matière de sécurité technique (RSSI, correspondant informatique et SSI, utilisateur de l'outil informatique, formateurs et autres personnels pouvant jouer le rôle de relais auprès des utilisateurs).

! Prérequis

Aucun prérequis

Thématique

Sécurisation du poste de travail, introduction à la cryptographie, sécurité d'Internet et de la messagerie, risques liés au nomadisme, sécurité du SI face aux risques de compromission des postes de travail.

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Certificats Electroniques

Réf. 6	Durée. 2,5 jours	En présentiel (TP)

Présentation

Cette formation offre un apprentissage de base en cryptographie, de connaitre le cadre juridique, réglementaire et ses référentiels documentaires. Celle-ci permettra également de traiter ce qui à trait aux maquettes et à la modélisation d'une IGC.

Objectifs

Comprendre la place des certificats électroniques dans la sécurité des systèmes d'information et les mécanismes à la base des infrastructures de gestion de clés. Connaître les règles de l'art et les obligations légales et réglementaires. Appréhender la mise en œuvre d'une IGC.

Programme

Jurisprudence en lien avec la signature électronique :

* Evolution du cadre juridique sur la signature électronique ;
* Qu'est-ce qu'une signature électronique en droit ?
* Exemples jurisprudentiels autour de la signature électronique et des écrits électroniques ;
* Notions de cachet et de copies électroniques.

Cadre règlementaire :

* Présentation du règlement européen eIDAS ;
* Présentation du Référentiel général de sécurité (RGS) ;
* La méthodologie de mise en conformité à ces deux règlementations ;
* La qualification eIDAS et RGS et comment recourir aux offres des prestataires qualifiés.

Référentiel documentaire d'une IGC :

* Savoir ce qu'est une politique de certification et son contenu ;
* Les conditions générales d'utilisation d'un service de signature électronique ;
* Les autres documents qui doivent être publiés tel que les certificats d'AC, les listes de révocations, les répondeurs OCSP ;
* Les documents à accès restreint tel que la déclaration des pratiques de certification, l'analyse de risque etc.

Fondements techniques :

* Introduction à la cryptographie ;
* Présentation du certificat électronique : principe, norme technique, enjeux de sécurité ;
* Présentation d'une Infrastructure de Gestion de Clé (IGC) : structure, bonnes pratiques, enjeux de sécurité ;
* Mise en œuvre pratique d'une IGC.

Niveau

Perfectionnement

Public

Personne s'intéressant à tout ce qui a trait à la signature électronique.

RSSI ou chefs de projet appelés à déterminer le besoin d'utiliser des certificats électroniques ou à piloter la mise en œuvre d'une infrastructure de gestion de clés.

Prérequis

Aucun prérequis

Thématique

Infrastructure de gestion de clé, crypto, signature électronique, RGS, eIDAS

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Internet et la Sécurité

Réf. 7a | **Durée. 5 jours** | **Présentiel ou Distanciel**

Objectifs

* Savoir mettre en œuvre des bonnes pratiques d'administration sécurisée d'un système d'information ;
* Connaître les principes de sécurisation liés aux différents éléments d'un système d'information : protocoles et filtrage réseau, systèmes d'exploitation et applications ;
* Appréhender les mécanismes de sécurité proposés par la cryptographie afin de savoir faire les bons choix dans la mise en œuvre de protocoles

Programme

* Pratiques d'administration : sécurité des postes et des réseaux d'administration, gestion des mots de passe, bonnes pratiques générales, cas concrets ;
* Sécurité des protocoles réseau TCP/IP et durcissement d'équipements réseau de type commutateur ou routeur ;
* Filtrage réseau et applicatif : pare-feu, relais (proxy) ;
* Architecture : principes et exemples d'architectures sécurisées ;
* Cryptologie appliquée : chiffrement, protection en intégrité, authentification et échange de secrets ;
* Protocoles sécurisés (TLS, IPsec et SSH) : objectifs et mécanismes de sécurité, cas d'usage pratiques ;
* Sécurité Wifi ;
* Web : protocoles et risques liés, exemples de vulnérabilités, mécanismes d'authentification, sécurisation d'un serveur ;
* Systèmes d'exploitation (Windows et Linux) : mécanismes de sécurité intégrés, durcissement et administration ;
* Active Directory : risques liés à l'administration, modèle de délégation de droits, GPO et durcissement.

Niveau

Perfectionnement

Public

Administrateurs système et réseau, confrontés aux problématiques de sécurisation des systèmes d'information.

Prérequis

Administration système et réseau

Thématique

Durcissement système, réseau et web

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Principes et organisation des audits en sécurité des systèmes d'information

Réf. 8a | **Durée. 2 jours** | **Présentiel ou Distanciel**

Présentation

Initier le public aux méthodes d'audit de sécurité d'un système d'information. Cette formation s'articule en plusieurs thèmes allant de l'audit de sécurité organisationnel et physique à l'audit de sécurité technique.

Objectifs

Permettre de superviser la réalisation d'un audit technique, de pouvoir organiser et choisir différentes prestations d'audit (type de prestation, périmètre, etc.).

Programme

* Introduction aux méthodes d'audit technique de la sécurité d'un système d'information (expertise sécurité) ;
* Apprentissage d'une méthodologie d'audit générique ainsi que des procédures : intégration de l'audit dans la gestion des risques SSI, étapes de réalisation d'un audit SSI, suivi d'un audit SSI ;
* Etude de cas de l'audit technique d'un système d'information : présentation d'un test d'intrusion, audit d'architecture et de configuration, audit applicatif et démos ;
* Sécurité et développement logiciel : cycle de développement, exigences de sécurité, conception, développement, tests et validation, déploiement, supervision, cas des prestataires, gestion des vulnérabilités ;
* Entretiens en audit SSI : comment poser les questions, les acteurs rencontrés et plusieurs fiches "pense-bêtes" ;
* Sécurité physique : protection environnementale (incendie, énergie, risque industriel, risque électromagnétique), contrôle d'accès (mécanique, logique), risque d'intrusion (protection périphérique, périmétrique et intérieure) ;
* Fourniture des listes techniques de points à vérifier pour les différents domaines.

Niveau

Perfectionnement

Public

Auditeurs SSI, Responsables de sécurité devant superviser des audits de sécurité de système d'information. Responsables administratifs soucieux d'utiliser les résultats des audits.

Prérequis

Aucun prérequis

Thématique

Méthodologie générale des audits en SSI.

Approche organisationnelle

Analyse de la sécurité physique et logique d'un système d'information.

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Audit technique en sécurité des systèmes d'information

Réf. 8b | **Durée. 5 jours** | **En présentiel (TP)**

Un questionnaire de sélection vous sera adressé avant le stage.

Présentation

La formation se déroule sous forme de travaux pratiques simulant la réalisation d'audits techniques sous différents aspects (réseau, système, applicatif).

Objectifs

Savoir réaliser un audit de sécurité élémentaire;
Savoir plus précisément ce qu'est une attaque informatique.

Programme

* Découverte réseau (balayages, reconnaissance, ...) ;
* Analyse d'équipement réseau (commutateur, routeur, pare-feu, ..);
* Audit Linux (mises à jour, élévations de privilèges, permissions, configurations, ...) ;
* Audit Windows/Active Directory (configuration AD, gestion des droits, récupération de secrets, attaques, ...) ;
* Audit Web (injections SQL, XSS, CSRF, ...) ;
* Test d'intrusion (outils, etude de cas, ...).

Niveau

Expert

Public

Personnes ayant de bonnes connaissances techniques

! Prérequis

Avoir suivi le stage 7a :

Internet et la Sécurité

Thématique

Audit (système, réseau, applicatif, AD), test d'intrusion

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité des applications Web

Réf. 9 | **Durée. 5 jours** | **Présentiel ou Distanciel**

Un questionnaire de sélection vous sera adressé avant le stage.

Objectifs

Améliorer la sécurité des applications web par une sensibilisation aux risques liés aux applications web, ainsi que par une prise de connaissance des bonnes pratiques de la SSI et de leurs déclinaisons dans le contexte web.

Programme

* Concepts de la gestion des risques et grands principes de la méthode EBIOS Risk Manager ;
* Identification du socle de sécurité ;
* Description des événements redoutés, identification des impacts et de la gravité ;
* Prise en compte de la notion d'écosystème ;
* Élaboration des scénarios stratégiques et opérationnels ;
* Traitement des risques et mesures de sécurité ;
* Amélioration continue de la sécurité et mise en place du cadre de suivi des risques.

Niveau

Perfectionnement

Public

Développeurs d'applications web

Une connaissance superficielle de PHP est souhaitable, mais les recommandations fournies ne sont pas spécifiques à ce langage et sont applicables dans d'autres langages.

! Prérequis

Serveurs web, base de données, développement, Linux

Thématique

Expertise technique

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Cryptographie

Réf. 10 | **Durée. 19 jours** | **Présentiel ou Distanciel**

Présentation

L'objectif de cette formation longue (4 semaines) est d'aborder tous les concepts fondamentaux de la cryptographie moderne (cryptographie symétrique et asymétrique), en étudiant les briques de base et en travaillant progressivement sur des structures plus avancées.

Objectifs

Former des personnels destinés à assurer le déploiement de technologies de sécurisation basées sur la cryptographie.

Aider à comprendre la nature des menaces, les raisonnements cryptographiques, et la justification des pratiques et des règles.

Programme

* Rappels mathématiques, notions de sécurité, algorithmique pour la cryptographie, problèmes difficiles,
* Chiffrement par bloc, chiffrement par flot, fonctions de hachage, modes opératoires de chiffrement, MAC, chiffrement authentifié,
* Chiffrement à clé publique, signature électronique, authentification et échange de clés,
* Génération d'aléa,
* Notions de cryptanalyse (symétrique et asymétrique),
* Preuves à divulgation nulle de connaissance,
* Cryptographie quantique et cryptographie post-quantique,
* Protocoles cryptographiques (partage de secret, vote électronique),
* Produits cryptographiques : cryptographie dans les protocoles de communication, gestion de mots de passe,
* Cryptomonnaie,
* Gestion des clés, infrastructure de gestion de clés publiques,
* Critères et schémas d'évaluation/certification, évaluation des équipements cryptographiques,
* Présentation du référentiel cryptographique, droit et réglementation de la SSI, la CNIL, droit et réglementation de la cryptologie.

Niveau

Expert

Public

Formation scientifique

! Prérequis

Avoir des prérequis en mathématiques.

Néanmoins, certains rappels seront faits durant cette formation.

Thématique

Confidentialité, intégrité, authentification (chiffrement, signature).

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité des réseaux sans fils

Réf. 11a | **Durée. 4 jours** | **Présentiel ou Distanciel**

Objectifs

Présenter :

* les technologies sans-fil et les architectures associées ;
* les risques relatifs à l'usage de réseau sans fil ;

Programme

* Wifi (IEEE 802.11) : les diverses normes, les architectures de réseaux, les évolutions, les vulnérabilités et parades ;
* Sécurisation d'un réseau sans fil ;
* Bluetooth ;
* Sécurité des réseaux mobiles de la 2G à la 5G ;
* Divers : RFID, géo-positionnement.

Niveau

Perfectionnement

Public

Administrateurs réseau et informaticiens possédant une expérience du déploiement de réseaux.

Prérequis

Aucun prérequis

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Homologation Sécurité

Réf. 12 | **Durée. 2 jours** | **Présentiel ou Distanciel**

Objectifs

Savoir bâtir et conduire un processus d'homologation ;
Savoir constituer un dossier d'homologation ;
Savoir motiver la prise de décision d'homologation ;
Comprendre la démarche d'homologation et son inscription dans le cadre réglementaire.

Programme

* Le processus d'homologation ;
* Ce stage inclut un rappel sur la méthode EBIOS Risk Manager.

Niveau

Perfectionnement

Public

Personnes devant mener ou accompagner un processus d'homologation, et qui pilotent en maîtrise d'ouvrage le management du risque. Stage s'adressant en particulier aux RSSI.

Prérequis

Aucun prérequis

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Incidents de Sécurité

Réf. 14 | **Durée. 4 jours** | **En présentiel (TP)**

Un questionnaire de sélection vous sera adressé avant le stage.

Présentation

Présenter les différentes phases d'une réponse à incident, et en particulier, permettre d'aborder la capture et l'exploitation des traces numériques présentes sous Windows et sur le réseau.

Objectifs

Être capable d'appréhender les différentes phases du traitement d'incidents de sécurité en ayant les bons réflexes et en utilisant des outils adaptés, notamment lors de la qualification / analyse d'un système compromis.

Programme

* Aspects légaux ;
* Gestion des incidents ;
* Collecte d'un système Windows ;
* Analyse d'un système Windows ;
* Analyse d'un fichier malveillant ;
* Analyse réseau ;
* Mise en pratique.

Niveau

Perfectionnement

Public

Administrateur de systèmes et réseaux, Analyste SOC, pilote technique de réponse à incident.

Prérequis

Informatique administration, connaissance de la ligne de commande UNIX.

Thématique

Incidents de sécurité, analyse d'un système Windows, analyse réseau

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Intégrer la sécurité numérique dans le projets SI de l'Etat

Réf. 16	Durée. 2 jours	Présentiel ou Distanciel

Objectifs

Donner les clés de compréhension, éléments de langage et outils méthodologiques pour intégrer les enjeux de la cybersécurité sur tout le cycle de vie d'un projet numérique, et ce dès la phase de cadrage et de faisabilité. Cette formation se veut concrète et pratique, et propose une boite à outils à destination des chefs de projets ou des directions de projets, désireux d'intégrer la composante cybersécurité dans leur démarche de gestion de projet et d'analyse de la valeur.

Programme

* Les enjeux de la cybersécurité pour un SI de l'État ;
* Le rôle du chef de projet comme garant de leur déclinaison et de leur juste valorisation ;
* L'organisation de l'État pour la sécurité du numérique et les acteurs clés sur un projet type ;
* Les différents textes réglementaires et leurs cas d'usage selon la nature du projet ;
* Les éléments essentiels de cadrage du volet sécurité du numérique en phase initiale d'un projet ;
* Déployer la démarche sur tout le cycle de vie projet/système dans le cadre d'une homologation de sécurité ;
* Adapter la démarche à une approche Agile ;
* Les guides et outils ANSSI à votre disposition.

Niveau

Perfectionnement

Public

Chefs de projet, responsables de directions de projets ou ingénieurs SIC amenés à intégrer le volet cybersécurité dans leur organisation projet ou dans leur processus de conduite de projet.

Représentants d'autorités administratives ou qualifiées de la SSI souhaitant affiner leurs connaissances et pratiques de l'homologation.

Prérequis

Gestion de projet

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Responsable de la Sécurité des systèmes d'information (RSSI) Aspects théoriques et réglementaires

Réf. 17a | **Durée. 5 jours** | **Présentiel ou Distanciel**

Présentation

Former les RSSI aux enjeux théoriques et règlementaires associés à leur métier. Cette formation peut ensuite être complétée par le stage 17b, qui se focalise sur des aspects plus techniques associés au métier de RSSI.

Objectifs

Fournir un socle de connaissances sur la gestion de la sécurité des systèmes d'information ;
Présenter les principaux enjeux de la sécurité des systèmes d'information ainsi que les règlementations associées ;
Présenter les principales mesures de sécurité et méthodes utiles à la fonction de RSSI.

Programme

* Retex RSSI ;
* Présentations de l'environnement cyber : aspects légaux, panorama des menaces ;
* Bases de gestion d'incidents de sécurité ;
* Démarches d'homologation ;
* Gestion des risques (EBIOS Risk Manager) ;
* Evaluation ;
* Certification ;
* Qualification.

Niveau

Perfectionnement

Public

RSSI, DSI, chef de projet

Prérequis

Aucun prérequis

Thématique

Théorie de la sécurité des systèmes d'information

Règlementations de la sécurité des systèmes d'information

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Responsable de la Sécurité des systèmes d'information (RSSI) Aspects techniques

Réf. 17b	Durée. 5 jours	Présentiel ou Distanciel

Objectifs

Approfondir les connaissances dans la gestion de la sécurité des systèmes d'informations,

Prendre davantage en compte le contexte juridique et réglementaire et les risques dans l'intégration de la SSI dans les projets.

Programme

* Architecture sécurisée ;
* VOIP ;
* Sécurité des systèmes industriels ;
* Sécurité et développement logiciel ;
* Déploiement IGC ;
* Audit SSI ;
* Codes malveillants et traces informatiques ;
* Système de détection d'intrusion.

Niveau

Perfectionnement

Public

RSSI, chef de projets, DSI.

! Prérequis

Aucun prérequis

Complémentaire au stage 17a. Responsable de la sécurité des systèmes d'information (RSSI - Aspects théoriques et réglementaires)

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Enjeux Stratégiques de la Cybersécurité

Réf. 18	Durée. 3 jours	Présentiel ou Distanciel

Présentation

Dans un contexte de numérisation croissante de la société et de l'économie, face à une montée de la conflictualité dans le cyberespace, ce stage permet d'avoir conscience des enjeux structurants de la Cybersécurité.

Objectifs

Il aborde en particulier les sujets d'attention de la Cybersécurité et les politiques publiques mises en place afin de protéger la société, que ce soit sous l'angle national ou international.

Programme

* Présentation du cyberespace : ses caractéristiques, ses tendances, ses acteurs stratégiques ;
* État de la menace d'origine cyber : attaquants, motivations, tendances, finalités, modes opératoires ;
* Cyberdéfense : gouvernance (gestion des risques, documentation), protection (architecture, mesures de sécurité), défense (détection, gestion des incidents) et résilience (continuité d'activité, gestion de crise) ;
* Modèle français : comment l'État organise la protection des systèmes d'information et le suivi des politiques publiques de cybersécurité ;
* Enjeux internationaux : sécurité collective et stabilité du cyberespace, coopérations, alliances, rôle des organisations internationales (UE, ONU, OTAN…).

Niveau

Initiation

Public

Décideurs, cadres et conseillers intervenant sur des enjeux de politique publique susceptibles d'inclure des aspects de sécurité numérique, et souhaitant disposer d'une vision globale sur les enjeux stratégiques liés à la cybersécurité.

! Prérequis

Aucun prérequis

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité des systèmes industriels

Réf. 19	Durée. 4 jours	Présentiel

Objectifs

Comprendre les enjeux liés à la cybersécurité des systèmes industriels et les particularités de ce domaine.
Être capable de mettre en œuvre un projet de renforcement du niveau de sécurité d'un système industriel.
Savoir programmer et sécuriser un automate industriel.

Programme

Jour 1
Introduction aux systèmes industriels et programmation d'un automate industriel ;

Jour 2
La cybersécurité des systèmes industriels et travaux pratiques ;

Jour 3
Projet de sécurisation d'un système industriel ;

Jour 4
Pas encore mis en œuvre, en cours d'évolution. (futur thème : sécurisation périmétrique d'un système industriel).

Niveau

Initiation

Public

Personnes en charge de la conception, du développement, de l'intégration, de l'exploitation ou de la maintenance de systèmes industriels (maîtrise d'ouvrage, maîtrise d'œuvre, exploitants, intégrateurs, etc.) ainsi qu'aux personnes amenées à réaliser des audits ou à accompagner des industriels dans leurs projets de renforcement de la sécurité des systèmes industriels.

Prérequis

Disposer de l'équivalent du 5a. Utiliser l'outil informatique de manière sécurisée

Thématique

Introduction aux systèmes industriels ; Sécurité des systèmes industriels ; Projet de sécurisation d'un système industriel.

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Cloud Computing enjeux de sécurité

Réf. 20 | **Durée. 2 jours** | **Présentiel ou Distanciel**

Présentation

Comprendre le Cloud Computing, ses enjeux, ses risques, les bonnes pratiques de sécurisation et la posture technique de l'agence

Objectifs

Comprendre les risques et les enjeux relatifs à l'usage du Cloud ;

Se familiariser avec SecNumCloud ;

Comprendre les recommandations de l'ANSSI relatives au Cloud.

Programme

* Introduction au Cloud Computing (définition, risques) ;
* Les apports de la qualification SecNumCloud ;
* L'architecture technique d'un cloud (les principale briques, leurs rôles et problématiques de sécurité associées) ;
* Le développement dans un environnement Cloud (DEVOPS, CI/CD) ;
* La sécurisation des API (celles du Cloud Provider et celles de vos services) ;
* L'IaC pour sécuriser l'infrastructure ;
* La gestion des secrets dans le Cloud (gestion des clés, chiffrement, coffre fort numérique) ;
* L'orchestration ;
* Les pratiques d'administration ;
* Conclusion.

NOUVEAU

Niveau

Perfectionnement

Public

Architectes, personnels techniques, des développeurs, des administrateurs, des RSSI.

! Prérequis

Connaissances générales du fonctionnement du Cloud Computing (mutualisation, virtualisation)

Principe d'usage d'un Cloud

Guide d'hygiène de l'ANSSI (notamment l'administration, le MCO et MCS)

Connaissances sur le fonctionnement d'un Système d'information (zones, cloisonnement, réseau, système, stockage, etc.)

Connaissances sur les pratiques de développement en environnement Cloud.

Thématique

Enjeux techniques de sécurité, l'architecture technique, la sécurité du développement.

Administration sécurisée Windows

Réf. 21 | **Durée. 5 jours** | **En présentiel (TP)**

Présentation

Présenter les bonnes méthodes d'administration ainsi que les fonctionnalités et technologies permettant la gestion sécurisée d'un parc Windows.

Objectifs

Présenter aux administrateurs les pratiques à bannir et celles à privilégier ;

Faire un panorama des fonctions et outils qui permettent d'augmenter le niveau de sécurité d'un parc Windows ;

Proposer une solution simple de journalisation.

Programme

Durant la formation, les principes de la défense en profondeur seront développés en détaillant les mécanismes qui peuvent être mis en place aux différents niveaux

Partie I

* Le réseau (accès, segmentation, sécurisation, supervision)
* Le poste de travail (phase de démarrage, chiffrement de données, la sécurité de base, supervision)
* Les comptes utilisateurs (jeton d'accès, comptes de service, comptes locaux, cycle de vie)
* L'authentification (LM/NTLM/Kerberos, les attaques et le multifacteur
* Les mots de passe (robustesse, verrouillage, stockage)

Partie II

* Les administrateurs (séparation par périmètre ; délégation, administration en tiers et bonnes pratiques)
* Leurs postes de travail (poste dédié, durci et leur gestion)
* Le réseau d'administration (réseau distinct, serveurs de rebonds)

Partie III

* La journalisation sera également couverte (centralisation d'événements, choix des événements, sysmon).

NOUVEAU

Niveau

Perfectionnement

Public

Administrateurs système, administrateurs réseau et architectes.

! Prérequis

Aucun prérequis mais une connaissance minimum de l'Active Directory et des stratégies de groupes est nécessaire.

Thématique

La sécurité du réseau, la sécurité du système, l'administration sécurisée et la journalisation

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Incubateur de CSIRT

Réf. 22 | **Durée. 15 jours** | **En distanciel**

Présentation

Le parcours d'incubation des CSIRT est un ensemble d'ateliers axés opérationnel et organisationnel, qui inclut également des visites ou des présentations par des acteurs importants du dispositif national cyber, telles que les forces de l'ordre, ACYMA ou des CSIRT sectoriels. La majorité des ateliers sont en distanciel mais certains d'entre eux se feront à la Tour Mercure ou dans une des salles du CFSSI au Campus Cyber.

Objectifs

Les objectifs de la formation sont de donner aux participants une vue d'ensemble sur les métiers d'un CSIRT, de partager l'expérience du CERT-FR et des acteurs de la communauté des CSIRT sur les services que devront mettre en oeuvre les CSIRT régionaux, et enfin de leur permettre de rencontrer des acteurs importants pour leurs missions. Ce parcours est ainsi principalement orienté pour des responsables CSIRT mais des analystes peuvent également y participer.

Programme

Jours 1 à 5

* Lancement; Promotion du CSIRT ; Culture CSIRT
* Dispositif national de crise ; Le CERT-FR et le cadre réglementaire
* Communication du CSIRT ; La RFC 2350 ; Coopération et réseaux de CSIRT
* Enjeux RH dans un CSIRT ; Chaine de traitement et matrice d'engagement
* Cas pratiques d'application de la matrice d'engagement ; Interactions avec la Division Réponse ; Interactions avec la Division Connaissance et Anticipation ; Premier niveau de réponse à incident

Jours 6 à 10

* Suivi d'un incident avec un prestataire ; Veille en vulnérabilités et publication d'alertes
* Capitalisation et partage de marqueurs ; Services DCA vers les opérateurs réglementés ; Logigramme de réponse à incident et exercices pratiques
* Fiches réflexes de réponse à incident ; Exercices pratiques - fiches réflexes réponse à incident ; Enjeux juridiques dans un CSIRT
* ComCyberGend ; Police Judiciaire ; Démarche qualité et d'amélioration continue
* Référentiel d'autoévaluation SIM3 ; Atelier DGSI

Jour 11 à 15

* MISP ; Outils de communication chiffrés
* Communication de crise ; La CNIL

NOUVEAU

Niveau

Initiation

Public / Prérequis

Personnel des CSIRT régionaux, profil responsable ou analyste

Pas de prérequis.

Thématique

Réponse à incident, Organisation CSIRT, Coopération

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité physique et logique des composants

Réf. 23	Durée. 5 jours	Présentiel (TP)

Présentation

Comprendre les notions de sécurité autour du composant et ses usages. Connaître les menaces et les manières de s'en protéger. Découvrir les garanties offertes par la certification.

Objectifs

Comprendre les menaces qui pèsent sur les implantations matérielles (cartes à puce, microcontrôleurs, systèmes embarqués, etc.).
Suivre l'état de l'art sur les protections ou les contre-mesures existantes et connaître les outils permettant d'évaluer leur efficacité.
Connaître les problématiques d'évaluation de la sécurité.

Programme

* Introduction à la sécurité des composants ;
* Aperçu du marché des composants ;
* Standards crypto et attaque ROCA ;
* Canaux auxiliaires et développement sécurisé ;
* Javacard comme exemple de carte ouverte ;
* La sécurisation des FPGA ;
* Les attaques par cache ;
* Attaques par injection de fautes (Cours+démo) ;
* Attaques invasives ;
* Certification des composants.

Niveau

Expert

Public

Spécialistes en électronique, en cryptographie, intégrateurs, architectes ou responsables d'une maîtrise d'ouvrage devant prendre en compte les questions de sécurité des implantations matérielles.

Prérequis

Connaissances en implémentations embarquées et/ou cryptographie

Thématique

Panorama des menaces sur les composants du logiciel au matériel

Attaques par observation et par injection de faute

Protection et évaluation des composants.

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Analyse de vulnérabilités logiciels

Réf. 24 | **Durée. 5 jours** | **Présentiel ou Distanciel**

Présentation

Présenter des techniques modernes d'exploitation de vulnérabilités utilisées par les attaquants.

Objectifs

Comprendre les techniques utilisées pour exploiter une vulnérabilité
Savoir réaliser une analyse statique et dynamique d'un code malveillant

Programme

* Mode opératoire des attaquants ;
* ASM x86-x64 ;
* Exploitation d'un buffer overflow sous Linux ;
* GDB ;
* Shellcode ;
* Présentation des contre-mesures historiques : ASLR, DEP ;
* Technique de contournement des protections : return-to-libc, ROP ;
* Exploitation sous Windows : Windbg, SEH ;
* Architecture système : espace noyau et espace utilisateur, MMU, Processus et Sandbox ;
* Architecture d'un navigateur web ;
* Présentation des contre-mesures modernes : ACG, XFG, CET, PAC ;
* Exploitation du navigateur : Use-After-Free et Confusion de type.

NOUVEAU

Niveau

Expert

Public

Ingénieurs en investigation numérique, Auditeur SSI

Analyste de code malveillant, Analyste SOC

Prérequis

Rétro-ingénierie x86-x64

Outils de debogage

Mode opératoire des attaquants

Thématique

Vulnérabilités logiciels : Buffer overflow, Use-After-Free, Confusion de type

Techniques d'exploitations et contre-mesures : ASLR, DEP, CFG, ROP, Shellcode

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité des systèmes embarqués

Réf. 25 | **Durée. 3 jours** | **Présentiel ou Distanciel**

Présentation

Cette formation est dédiée à l'étude des menaces pour la sécurité de l'information traitée par des équipements électroniques qui existent lorsque l'on considère que l'attaquant peut disposer d'un accès physique aux équipements.

Objectifs

Comprendre les menaces (physiques et logiques) qui pèsent sur les implantations matérielles (systèmes embarqués, etc.).
Identifier les vecteurs de compromission de la sécurité des systèmes embarqués pour mieux en appréhender la conception ou l'analyse.
Suivre l'état de l'art sur les protections ou les contre-mesures existantes et connaître les outils permettant d'évaluer leur efficacité.

Programme

* Eléments matériels et architecture des SoC : Introduction aux systèmes embarqués, éléments d'architecture, enjeux de sécurité,
* Outils et techniques d'analyse : Introduction à la rétroconception matérielle, menaces et profils d'attaquant,
* Interfaces et protocoles de communication : Stratégies d'analyse et d'interaction avec les composants via leurs interfaces de communication,
* Enjeux pour l'investigation numérique : Méthodes d'analyse et d'exploitation de la sécurité matérielle dans le contexte de l'investigation numérique, compromis auditabilité/sécurité,
* Chaine de démarrage sécurisée : Panorama des méthodes de sécurisation du démarrage, sur SoC et CPU,
* Evolution de la sécurité : Etudes de cas réels à fort enjeu de sécurité illustrant des successions de phases attaque-défense,
* Introduction aux attaques sur composants : Vulnérabilités résiduelles impactant les composants.

Niveau

Expert

Public

Intégrateurs, architectes, spécialistes d'une maîtrise d'ouvrage devant prendre en compte les questions de sécurité des systèmes embarqués, spécialistes en tests d'intrusion.

Prérequis

Connaissances de base en informatique

Connaissances de base en SSI

Thématique

Eléments d'architecture des systèmes embarqués - Démarrage sécurisé - Attaques par accès physique

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité des architectures virtualisées

Réf. 26 | **Durée. 3 jours** | **Présentiel ou Distanciel**

Présentation

Cette formation vise à présenter les enjeux de sécurité et promouvoir les bonnes pratiques liés à l'utilisation des technologies de virtualisation. Une démarche est également préconisée pour concevoir des architectures sécurisées mettant en œuvre ces technologies.

Objectifs

Connaître les technologies et principes sous-jacents à la virtualisation,
Être sensibilisé aux risques et connaître les bonnes pratiques liées à la mise en œuvre de la virtualisation,
S'approprier une démarche de sécurisation des architectures virtualisées.

Programme

* Introduction aux technologies de virtualisation (virtualisation complète, paravirtualisation, VT-X, VT-D, hyperviseurs types 1 et type 2, conteneurs) ;
* Virtualisation du poste de travail (locale ou distante) ;
* Virtualisation des serveurs ;
* Virtualisation du réseau (vSwitch, D-vSwitch, SDN, VXLAN, NSX) ;
* Virtualisation du stockage (mode bloc, mode fichiers) et chiffrement ;
* Gestion de la virtualisation dans un Datacenter ;
* Introduction aux architectures de cloud computing ;
* Etudes de cas.

Niveau

Perfectionnement

Public

Architectes sécurité

Responsables sécurité

Administrateurs

Prérequis

Aucun Prérequis

Thématique

Technologies de virtualisation

Architectures virtualisées

Risques et bonnes pratiques liés à la virtualisation

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Sécurité firmware et chaîne de démarrage

Réf. 27 | **Durée. 3 jours** | **Présentiel ou Distanciel**

Présentation

Cette formation présente la chaîne de démarrage d'un ordinateur, de la mise sous tension à l'initialisation du système d'exploitation. Elle détaille les mécanismes de sécurité permettant d'assurer l'intégrité des composants tout au long de la chaîne, leur utilisation pour la confidentialité des données du système, leur mise à jour et leur vérification par une entité tierce. Le cours s'appuie sur plusieurs études de cas concrets et de vulnérabilités passées, et fournit les connaissances nécessaires aux stagiaires pour développer une politique de sécurité contre des attaques locales et distantes de la chaîne de démarrage.

Objectifs

Vue détaillée des différents composants logiciels de la chaîne de démarrage (de l'initialisation du matériel au démarrage du système d'exploitation). Le rôle des composants matériels comme racine de confiance (coprocesseurs de sécurité et TPM). La confiance à accorder à chaque élément : vulnérabilités potentielles, risque associé, contre mesures. Les bonnes pratiques pour s'assurer du maintien d'un système en condition de sécurité. Les possibilités de durcissement des composants pour le cas de systèmes sensibles. L'utilisation d'attestation distante dans le cadre d'une approche Zero Trust.

Programme

* Elements de la chaine de démarrage : pre-boot, UEFI, bootloader, OS ;
* Pre-boot : Intel BootGuard, AMD PSP ;
* UEFI : structure et fonctionnalités (initialisation, boot services, runtime services, secured variables, SMM handlers) ;
* TPM : secured boot et measured boot, utilisation pour le scellement de secrets ;
* Racines de confiance : SRTM et DRTM ;
* Bootloader et OS : principes généraux et étude de cas (Windows, Chromebook, Linux/Grub/Trenchboot) ;
* Attestation distante : principes généraux et étude de cas (Windows Azure, Google Cloud, Linux/safeboot) ;
* Mise à jour : mécanismes (capsule UEFI, signatures) et étude de cas (Windows Update et Bitlocker, Linux LVFS). Risques sur la supply-chain et SBOM ;
* Recommandations sur la réduction de la surface d'attaque UEFI : options de compilation et de configuration ;
* Solutions de détection et supervision.

NOUVEAU

Niveau

Expert

Public

DSI, RSSI, Ingénieurs

Architecture d'un ordinateur (CPU, bus de communication, périphérique)

Prérequis

Principes de fonctionnement d'un programme binaire : chargement en mémoire, exécution

Thématique

Fonctionnement de la chaîne de démarrage x86/amd64

Mécanismes d'intégrité et de confidentialité

Mise à jour et chaîne d'approvisionnement (supply-chain)

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Gestion de crise (Volet opérationnel, Stratégique, Communication)

Réf. 29 | **Durée. 3 jours** | **Présentiel ou Distanciel**

Objectifs

Appréhender les enjeux de la gestion de crise cyber : comprendre les spécificités de la crise cyber et les impacts opérationnels/stratégiques pour une organisation ;
Connaître les « bonnes pratiques » de la gestion de crise cyber : niveau opérationnel et stratégique (avec un focus sur le volet communication) ;
Apprendre à mettre en place un dispositif de gestion de crise adapté aux enjeux cyber ;
Savoir réagir à une cyberattaque (dans le cadre d'une simulation exercice).

Programme

* Présentation des enjeux de la gestion de crise cyber ;
* Présentation des étapes d'une crise cyber ;
* Présentation des bonnes pratiques de gestion de crise cyber : en amont de la crise (préparation du dispositif cyber) et lors de la crise ;
* Présentation de plusieurs dispositifs de crise cyber (étatique (plan PIRANET), privé et public) : organisation, rôles, fonctions ;
* Exercice : simulation d'une gestion de crise cyber (niveau stratégique).

Niveau

Perfectionnement

Public

Personnes amenées à être mobilisées dans le cadre d'une gestion de crise cyber : fonctions décisionnelles, directions métiers, responsables de la sécurité, gestionnaires des risques, responsables de la continuité d'activité ou de la gestion de crise, responsables du numérique, responsable de la sécurité des systèmes d'information.

Prérequis

Aucun prérequis

Thématique

Gouvernance cybersécurité et maîtrise des risques

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

Analyste SOC

Réf. 30 | **Durée. 5 jours** | **En présentiel (TP)**

Présentation

La formation a pour objectif de rappeler les méthodologies du SOC mais également d'entrer dans le détail de la reconnaissance des attaques les plus régulièrement utilisées sous Windows. La méthodologie de travail consiste, pour chaque thème, à présenter la théorie puis la pratique de la démarche de recherche d'analyse, et de qualification des journaux pour préciser le contour de l'attaque. Ces analyses sont uniquement conduites à partir d'éléments à disposition d'un SOC (journaux, éventuellement EDR).

Objectifs

Reconnaître une attaque connue sous windows, caractériser cette attaque. Pouvoir produire des signatures sur les schémas connus voire sur de nouvelles méthodologies d'attaques.

Programme

Panorama de la détection système

Chaîne de détection et terminologie ; Organisation des équipes ; Sources de données ; Normalisation et standardisation des données ; Connaissance du SI supervisé et des pratiques d'administration ; Cycle de vie des signatures ; Tableaux de bord ; Environnement, contexte de détection, interaction avec les autres acteurs de la sécurité

Méthodologies

Kill chain / Mitre attack ; « Pyramide of pain » et détection de menace connue vs inconnue ; Démarche de création et de hiérarchisation des nouvelles alertes

Techniques de détection pour Windows

Détection grâce aux journaux d'authentification ; Techniques d'attaque et de détection Powershell ; Pré-requis et création de règles Sysmon ; Détection des techniques de latéralisation ; Détection de la persistance ; Repérage des traces générées par les outils communément utilisés par les attaquants ; Fonctionnement et détection des élévations de privilège ; Détection en amont de la reconnaissance faite par l'attaquant

Techniques de détection de compromission d'autres environnements

Linux ; Réseau

Processus métier des analystes

Processus d'investigation d'une alerte ; Processus de chasse (hunting)

NOUVEAU

Niveau

Perfectionnement

Public

Analystes SOC exploitant les alertes ou produisant de nouvelles alertes, soit nouvellement arrivés dans un SOC soit déjà présent.

Prérequis

Aucun prérequis

Thématique

Méthodologies du SOC et de l'analyste SOC

Méthodes de détection sous Windows

Méthodes de détection pour les autres plateformes

Plus d'informations :

www.ssi.gouv.fr/administration/formations/

CENTRE DE FORMATION À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Le CFSSI définit et met en oeuvre la politique de formation à la SSI de l'Agence nationale de la sécurité des sytèmes d'information (ANSSI). Situé au Campus Cyber, il propose :

- *des formations courtes dispensées par des experts de l'ANSSI ;*
- *un cycle long permettant d'obtenir le titre d'Expert en SSI ;*
- *plusieurs programmes et dispositifs visant à promouvoir la reconnaissance de formations continues ou initiales dans le domaine de la SSI.*

RETROUVEZ LES FORMATIONS, LES PROGRAMMES PARTENAIRES ET TOUTES LES INITIATIVES DU CFSSI SUR LE SITE DE L'ANSSI.

Plus d'informations : www.ssi.gouv.fr/administration/formations/

Version 2.0—Décembre 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr