RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Catalogue du centre de formation à la sécurité des systèmes d'information

2024

Catalogue du centre de formation à la sécurité des systèmes d'information

2024

Sommaire

Formations

Le centre de formation

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). Il définit et met en œuvre la politique de formation à la SSI de l'ANSSI.

1

Les formations courtes

Le CFSSI propose, chaque année, environ 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 un large choix de niveaux de technicité**, ces stages sont accessibles aux seuls agents de l'administration française : État, collectivités territoriales et fonction publique hospitalière, ainsi qu'aux membres des opérateurs d'importance vitale (OIV) et des opérateurs de service essentiel (OSE).

Le catalogue des formations courtes est disponible sur le site de l'ANSSI :
www.ssi.gouv.fr/administration/formations/catalogue-des-stages/

2

La formation longue : le titre ESSI

L'expert en sécurité des systèmes d'information (ESSI) **garantit la sécurité des systèmes d'information tout au long de leur cycle de vie**, en intervenant aux différentes étapes, depuis l'expression de besoin jusqu'à l'exploitation, en passant par le développement.

- Formation gratuite professionnalisante
- Titre ESSI : Expert en Sécurité des Systèmes d'Information
- Enregistré niveau 7 au répertoire national des certifications professionnelles
- Équivalence Bac+5

Plus d'informations sur le site de l'ANSSI :
www.ssi.gouv.administration/formations/titre-essi/

Le CFSSI définit et met en œuvre la politique de formation à la SSI de l'ANSSI.

3

Le MOOC SecNum*académie*

Dans le cadre de sa mission de sensibilisation, l'ANSSI propose SecNum*académie* pour former le plus grand nombre de citoyens à la sécurité du numérique.

Ce format de cours en ligne a pour objectif de **sensibiliser les utilisateurs en milieu professionnel à la sécurité du numérique** afin qu'ils deviennent acteurs de leur sécurité et de celle de leur entreprise.

Grâce à ce MOOC, les utilisateurs pourront apprendre et assimiler des notions de base de la sécurité des systèmes d'information (SSI) utiles au travail comme à la maison.

Chaque module aborde une thématique clé de la sécurité des systèmes d'information :

- **Module 1 :** panorama de la SSI
- **Module 2 :** sécurité de l'authentification
- **Module 3 :** sécurité sur Internet
- **Module 4 :** sécurité du poste de travail et nomadisme

Plus d'informations :
secnumacademie.gouv.fr

4

La labellisation SecNum*edu*

Le label SecNum*edu* a été créé par l'ANSSI pour **les formations spécialisées en sécurité informatique**.

Le label :

- **concerne les formations initiales** d'enseignement supérieur en cybersécurité ;
- **apporte une assurance** aux étudiants et aux employeurs sur le contenu de la formation ;
- **répond à une charte et à des critères** définis par l'ANSSI en collaboration avec les acteurs du domaine ;
- **améliore le référencement des formations en sécurité du numérique** par la mise en place d'un processus éprouvé ;
- **participe au renforcement et au développement des enseignements** en matière de sécurité du numérique.

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

5

La labellisation SecNum*edu* Formation Continue

Ce label, attribué pour 3 ans, concerne les formations continues d'enseignement supérieur en cybersécurité. Il permet ainsi de disposer d'une **liste des formations continues en sécurité du numérique**.

Les organismes de formation qui proposent la formation labellisée **s'engagent sur une charte**. La formation est inscrite au Répertoire Spécifique de France Compétences et/ou la formation se déclare conforme à un cahier des charges reconnu par l'ANSSI.

Fonctionnement des formations

Nous rappelons que :

- Les demandes de stages sont adressées par le ministère de tutelle dont relève le stagiaire ou sont 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.
- Le calendrier des formations est prévisionnel, celui-ci est susceptible d'évoluer en fonction des contraintes opérationnelles de l'ANSSI.

1

Les formations en présentiel :

La convocation

Une convocation à la session de formation est **adressée par mail**, avec le livret d'accueil et le programme de formation.

Les stagiaires sont tenus de **suivre toutes les séquences de formations**, avec assiduité et ponctualité, et sans interruption. Des feuilles de présence seront émargées par les stagiaires, par demi-journée et contresignées par l'intervenant.

Les horaires

Les formations commencent à 09h15 et finissent à 16h30.
La pause méridienne est de 1h30.

L'accueil du 1er jour

L'accueil du 1er jour se fera à l'entrée **du Campus Cyber** par une personne du Centre de formation.

Le QR code sur la convocation permettra de passer les portiques de sécurité et d'emprunter les ascenseurs.

Restauration et pause-café (8h-17h)

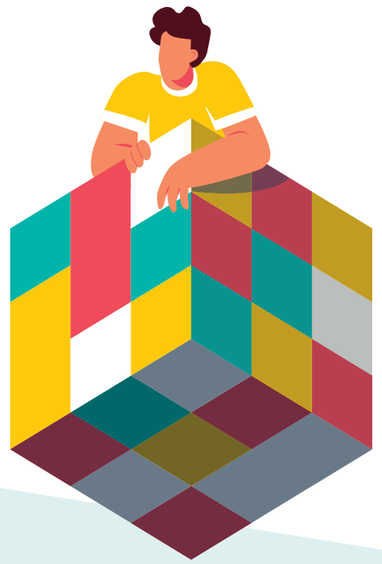
- **R+0, R+1 :**
  Cafétéria (Café, viennoiseries)
- **R+1 :**
  Food Court Nova (Restauration)
- **R+12 :**
  Espace café réservé aux stagiaires du CFSSI

2

Les formations à distance :

En cas de formation en distanciel, le guide de connexion à la plateforme de visioconférence est envoyé. **Aucune de nos formations ne sont enregistrées**.

En visioconférence, l'émargement est dématérialisé par l'envoi d'un mail à l'intervenant daté et signé par le stagiaire chaque demi-journée.



3

L'attestation de suivi :

À l'issue de l'action de formation et dans un délai d'un mois après celle-ci, le stagiaire recevra par mail une **attestation de suivi**, le lien pour le **support pédagogique du formateur** ainsi qu'un autre lien pour le **questionnaire d'évaluation** de formation.

Calendrier annuel

Niveaux

I Initiation P Perfectionnement E Expert

N°	STAGES	NIVEAU	TP	JOURS	JANV.	FÉV	MARS	AVRIL	MAI	JUIN	JUIL.	SEPT.	OCT.	NOV.	DÉC.
1	Panorama de la sécurité des systèmes d'information	I		1		27		2	6					12	2
2a	Premiers pas en Tempest	I		1				29					14		
2	Sécurité électromagnétique (Tempest)	P		5						10 - 14				25 - 29	
4	La Méthode EBIOS *Risk Manager*	P		2	29 - 30		5 - 6		13 - 14			16 - 17		4 - 5	9 - 10
5a	Utiliser l'outil informatique de manière sécurisée (Théorie)	I		2	22 - 23			29 - 30		24 - 25		2 - 3		4 - 5	
5b	Utiliser l'outil informatique de manière sécurisée (Pratique)	I	X	3	24 - 26					26 - 28		4 - 6		6 - 8	
6	Certificats électroniques	I	X	2.5				2 - 4		10 - 12					11 - 13
7a	Fondamentaux techniques de la sécurité des systèmes d'information	P		5			11 - 15						7 - 11		
8a	Principes et organisation des audits en sécurité des systèmes d'information	P		2	11 - 12			2 - 3	6 - 7			2 - 3			16 - 17
8b	Audit technique en sécurité des systèmes d'information	E	X	5		12 - 16				17 - 21			21 - 25	18 - 22	
9	Sécurité des applications Web	P		5			18 - 22							25 - 29	
10	Cryptographie	E		19	18 - 22	8 - 12 22 - 26	5 - 8								
11a	Sécurité des réseaux sans fils	P		4		5 - 8			27 - 30			16 - 19			
12	Homologation sécurité	P		1			25			1			21		
14	Incidents de sécurité	P	X	4			5 - 8	22 - 25				10 - 13	8 - 11		
16	Intégrer la sécurité numérique dans les projets SI de l'État	P		2				29 - 30				30/09 - 1/10			
17a	Responsable de la sécurité des systèmes d'information (RSSI) Aspects théoriques et réglementaires	P		5	15 - 19					3 - 7		16 - 20		18 - 22	
17b	Responsable de la sécurité des systèmes d'information (RSSI) - Aspects techniques	P		5		5 - 9				24 - 28		30/09 - 04/10			9 - 13
18	Enjeux stratégiques de la cybersécurité	I		3					22 - 24				14 - 16		
19	Sécurité des systèmes industriels	I		4	22 - 25			22 - 25				24 - 27		12 - 15	
20	*Cloud Computing* et DevOps : enjeux de sécurité	P		2				2 - 3						25 - 26	
21	Administration sécurisée Windows	P	X	5			18 - 22								16 - 20
23	Sécurité physique et logique des composants	E	X	5						3 - 7				25 - 29	
24	Analyse de code d'exploitation	E	X	5			26/02 - 01/03							2 - 6	
25	Sécurité des systèmes embarqués	E		3			25 - 27								
26	Sécurité des architectures virtualisées	P		3	15 - 17				27 - 29			9 - 11		12 - 14	
27	Sécurité firmware et chaîne de démarrage	E	X	5	29 - 2								14 - 18		
29	Gestion de crise (Volet opérationnel, Stratégique, Communication)	P		3						17 - 19					2 - 4
30	Analyste SOC	P	X	5				8 - 12			1 - 5				
31	Nouveau Réseau & Sécurité	E	X	5											
32	Nouveau Analyses statiques et dynamiques des architectures matérielles et logicielles	E	X	3											
33	Nouveau Enjeux de sécurité DevOps dans la gestion de configuration et de déploiement dans les SI	E	X	3											
34	Nouveau Sécurité des systèmes Linux	E	X	4											

Fiches de *formation*

Panorama de la sécurité des systèmes d'information

RÉFÉRENCE ***1***

DURÉE

1 jour

NIVEAU

Initiation

Public

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

Prérequis

Aucun prérequis.

Thématiques

Découverte de la cybersécurité.

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.

Premiers pas en TEMPEST

RÉFÉRENCE ***2a***

DURÉE

1 jour

NIVEAU

Initiation

Public

Toute personne amenée à traiter des informations classifiées.

Prérequis

Aucun prérequis.

Thématiques

Organisation des réglementations TEMPEST françaises et internationales ; moyens de protection contre la menace TEMPEST.

Présentation

Ce stage présente les menaces apportées par les ondes électromagnétiques en confidentialité (TEMPEST), mais aussi en intégrité et en disponibilité (AGREMI).

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

Les moyens de protection contre la menace TEMPEST sont abordés.

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 et la démarche de sécurisation.
- Le zonage TEMPEST.

Sécurité électromagnétique (TEMPEST)

RÉFÉRENCE **2**

DURÉE

5 jours
Présentiel

NIVEAU

Perfectionnement

Public

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

Les apprenants doivent être habilités au niveau SECRET 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.

Prérequis

Aucun prérequis nécessaire. Éventuellement avoir suivi la version courte du stage (référence 2a, Premiers pas en TEMPEST), mais sans obligation.

Thématiques

Réglementations TEMPEST françaises et internationales ; présentation des agressions électromagnétiques intentionnelles (AGREMI) ; ateliers pratiques.

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.

Comprendre la réglementation relative au domaine TEMPEST.

Programme

1er jour

- Présentation des menaces TEMPEST et AGREMI.
- Veille sources publiques.
- Rappels de physique.
- Aspects juridiques de la protection contre les SPC.

2ème jour

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

3ème jour

- AGREMI et Cyber-sécurité.
- Air-Gap.
- Les règles d'installation - 2ème partie.

4ème jour

- Cage de FARADAY Théorie.
- Ateliers pratiques.

5ème jour

- Mise en situation : étude de cas en groupe.
- TEMPEST appliqué aux systèmes.
- Bilan et conclusion.

La Méthode EBIOS Risk Manager

RÉFÉRENCE ***4***

DURÉE

2 jours

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.

Thématiques

Gouvernance cybersécurité et maîtrise des risques.

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 les décideurs et les acteurs opérationnels. 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.

Utiliser l'outil informatique de manière sécurisée (Théorie)

RÉFÉRENCE ***5a***

DURÉE

2 jours

NIVEAU

Initiation

Public

Personnes souhaitant découvrir macroscopiquement les aspects techniques et organisationnels de la cybersécurité : RSSI, correspondants informatiques et SSI, formateurs, et autres personnels pouvant jouer le rôle de relais auprès des utilisateurs.

Prérequis

Aucun prérequis.

Thématiques

Sécurité de la messagerie électronique, sécurité Web, sécurité du poste de travail.

Présentation

Cette formation informe 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.

Connaître les avantages et les limites des outils de sécurité aidant les utilisateurs à se 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.

Utiliser l'outil informatique de manière sécurisée (Pratique)

RÉFÉRENCE ***5b***

DURÉE

3 jours
Présentiel (TP)

NIVEAU

Initiation

Public

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

Prérequis

Aucun prérequis.

Thématiques

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.

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 de services numériques).

Programme

1er jour : 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 pare-feu, d'un anti-virus, d'un effaceur sécurisé.

2ème jour : Introduction à la cryptographie

Historique, différence entre chiffrement symétrique et asymétrique, objectifs de la cryptographie asymétrique, présentation de PGP et du chiffrement avec certificats.

3ème jour : 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, le fonctionnement d'un navigateur Internet et les bonnes pratiques de configuration.

4ème jour : 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.

5ème jour

Risques de sécurité liés au nomadisme (en environnement Microsoft) et aux mesures de sécurité qui permettent de les limiter, qu'il 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 pare-feu logiciel, de réutilisation de secrets d'authentification, etc.

Certificats électroniques

RÉFÉRENCE ***6***

DURÉE

2,5 jours
Présentiel (TP)

NIVEAU

Initiation

Public

Personne s'intéressant à tout ce qui a trait à la signature électronique et notamment les certificats électroniques, à la fois sur les plans techniques et réglementaires.

Le public cible sont des RSSI ou des 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.

Thématiques

Infrastructure de gestion de clés ; cryptographie ; signature électronique ; RGS ; eIDAS.

Présentation

Cette formation traite pour moitié des aspects techniques et pour moitié des aspects juridiques et réglementaires des certificats électroniques.

Elle offre un apprentissage de base en cryptographie et la modélisation d'une IGC (à la fois théorique et pratique) et permet également de traiter les cadres juridiques et réglementaires et les référentiels documentaires régissant l'utilisation des certificats électroniques.

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

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 (TP).

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 tels que la déclaration des pratiques de certification, l'analyse de risque etc.

Jurisprudence en lien avec la signature électronique :

- Évolution 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 copie électroniques.

Fondamentaux techniques de la sécurité des systèmes d'information

*RÉFÉRENCE **7a***

DURÉE

5 jours

NIVEAU

Perfectionnement

Public

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

Prérequis

Connaître l'administration système et réseau.

Thématiques

Durcissement système, réseau et web.

Objectifs

Savoir mettre en œuvre des bonnes pratiques de sécurisation d'un système d'information.

Connaître les principes de sécurisation liés aux différents éléments d'un système d'information : architecture, équipements de sécurité, 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 sécurisés.

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.
- Filtrages réseau et applicatif : pare-feu, relais (proxy).
- Architecture : définitions, 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.

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

*RÉFÉRENCE **8a***

DURÉE

2 jours

NIVEAU

Perfectionnement

Public

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

Prérequis

Aucun prérequis.

Thématiques

Méthodologie générale des audits en SSI ; approche organisationnelle ; analyse de la sécurité physique et logique d'un système d'information.

Présentation

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

Objectifs

Les compétences méthodologiques et pratiques obtenues en fin de stage doivent 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.
- Étude de cas de l'audit technique d'un système d'information.
- Sécurité et développement logiciel.
- Fourniture des listes techniques de points à vérifier pour les différents domaines.

Audit technique en sécurité des systèmes d'information

RÉFÉRENCE ***8b***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Expert

Public

Personnes ayant de bonnes connaissances techniques.

Prérequis

Avoir suivi le stage 7a (Fondamentaux techniques de la sécurité des systèmes d'information).

Thématiques

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

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

Sécurité des applications Web

RÉFÉRENCE ***9***

DURÉE

5 jours

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

Avoir une culture concernant les problèmes SSI rencontrés lors de la conception d'applications web permet de mieux apprécier et comprendre le contenu des cours.

Thématiques

Architectures web ; protocoles et interfaces ; authentification et standards.

Présentation

Cette formation sensibilise aux risques et aux problèmes de sécurité propres aux applications web. Elle aborde les bonnes pratiques de conception permettant, pour chacun des domaines incontournables pour les développeurs d'applications web, de réduire ces risques par une familiarisation aux vulnérabilités répandues, aux standards à implémenter et à l'écosystème qui entourent une application web.

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

1er jour

Introduction : Rappels sur HTTP, rappels sur la navigation web, menaces et scénarios d'attaque, objectifs de la formation.

Vulnérabilités : panorama des vulnérabilités, exemples concrets et techniques d'attaques pour compréhension des risques inhérents au web.

2ème jour

Architecture : déclinaison de trois études de cas en choix d'architectures fonctionnelle, logique et physique ; approche par le risque.

Architecture logicielle : bonnes pratiques de développement relatives à chacun des risques de l'OWASP Top 10.

Suite →

Sécurité des applications Web

Programme *(suite)*

3ème jour

Authentification et gestion des sessions : mécanismes d'authentification répandus sur le web, authentification multifacteur, maintien de sessions et cookies, stockage des mots de passe.

Single sign on : fonctionnement et bonnes pratiques liées à l'utilisation d'assertions SAML, aux protocoles OpenID Connect, CAS et Kerberos ; quiz intermédiaire.

4ème jour

Téléversement de fichiers : risques liés au téléversement (upload), au stockage et au téléchargement (download) de fichiers ; faiblesse de certaines mesures, grands principes de sécurité appliqués au téléversement, principes spécifiques web.

Services web : description d'interface, SOAP, REST ; dans ce contexte : mécanismes d'authentification, de protection de la donnée, du transport, attaques et bonnes pratiques sur l'implémentation.

5ème jour

Sécurité côté navigateur : attaques côté client, contraintes et fonctionnalités de sécurité de la plateforme web, SOP, XSS, CSRF, cookies, CORS.

Quiz final.

Cryptographie

RÉFÉRENCE ***10***

DURÉE

19 jours

NIVEAU

Expert

Public

Personnes ayant une formation scientifique.

Prérequis

Avoir quelques prérequis en mathématiques. Néanmoins, certains rappels seront faits durant cette formation.

Thématiques

Confidentialité ; intégrité ; authentification (chiffrement, signature).

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.

Sécurité des réseaux sans fils

*RÉFÉRENCE **11a***

DURÉE

4 jours

NIVEAU

Perfectionnement

Public

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

Prérequis

Aucun prérequis.

Thématiques

Sécurité du WI-FI ; sécurité des réseaux mobiles ; sécurité des autres protocoles de communication (Bluetooth, BLE, LoRaWAN, RFID, GNSS).

Présentation

Cette formation est dédiée à l'étude des menaces pour la sécurité de l'information traitée par des équipements électroniques et provenant de l'utilisation d'interfaces de communication radiofréquence.

Les menaces ciblant des protocoles de communication radio ou des équipements communicants sont introduits.

La sécurité de protocoles communément mis en œuvre pour assurer des services sensibles et omniprésents dans notre société (réseaux mobiles, GNSS, Wi-Fi, Bluetooth…) est analysée de manière à en identifier les garanties apportées et les limites.

Objectifs

Présenter :

- les technologies sans-fil et les architectures associées ;
- les risques relatifs à l'usage de réseau sans fil ;
- les contre-mesures disponibles et leurs limites.

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.

Homologation Sécurité

*RÉFÉRENCE **12***

DURÉE

1 jour

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.

Thématiques

Gouvernance cybersécurité et maîtrise des risques.

Présentation

Comprendre l'homologation de sécurité d'un système d'information et être capable de piloter l'homologation d'un SI.

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

L'approche pédagogique est la suivante :

- Définition des termes employés et présentation de la démarche.
- Exposé des contextes dans lesquels une homologation est obligatoire ; pourquoi est-ce recommandé dans tous les cas.
- Construction collective de l'organisation d'un projet d'homologation.
- Réflexion collective sur les leviers pour convaincre.
- Utilisation d'outils dans des cas fictifs.

Incidents de sécurité

RÉFÉRENCE ***14***

DURÉE

4 jours
Présentiel (TP)

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.

Thématiques

Incidents de sécurité ; analyse d'un système Windows ; analyse réseau.

Présentation

Cette formation présente les différentes phases d'une réponse à incident. En particulier, elle permet 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.

Intégrer la sécurité numérique dans les projets SI de l'État

RÉFÉRENCE ***16***

DURÉE

2 jours

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 (par obligation réglementaire dans le cadre d'une homologation, ou par nécessité liée à des enjeux sécuritaires particuliers).

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

Responsables de la conformité.

Prérequis

Gestion de projets.

Thématiques

Gouvernance cybersécurité et maîtrise des risques.

Présentation

Cette formation vise à donner les clés de compréhension, les éléments de langage et les 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.

Objectifs

Appréhender concrètement les enjeux et les besoins de sécurité numérique dans un projet.

Intégrer pleinement cette composante sur tout le cycle de vie d'un SI dès la phase de faisabilité et d'analyse de la valeur.

Cadrer et adapter la démarche de maîtrise du risque cyber au contexte et à la criticité du SI, en lien avec la réglementation, et particulièrement dans le cadre d'une démarche d'homologation.

Identifier les parties prenantes et leurs rôles.

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.
- Le cadre réglementaire relatif à la sécurité numérique.

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

*RÉFÉRENCE **17a***

DURÉE

5 jours

NIVEAU

Perfectionnement

Public

RSSI, DSI, chef de projets.

Prérequis

Aucun prérequis.

Thématiques

Théorie de la sécurité des systèmes d'information ; règlementations de la sécurité des systèmes d'information.

Présentation

Cette formation - destinée en priorité aux RSSI - vise à former ces derniers aux enjeux théoriques et règlementaires associés à leur métier. Cette formation peut ensuite être complétée par le stage 17b (Responsable de la Sécurité des systèmes d'information - Aspects techniques), 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, des méthodes et des réflexes qui seront utiles au quotidien.

Présenter les principaux enjeux de la sécurité des systèmes d'information ainsi que les règlementations associées.

Présenter les principales mesures de sécurité et les 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).
- Évaluation.
- Certification.
- Qualification.

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

*RÉFÉRENCE **17b***

DURÉE

5 jours

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).

Thématiques

Gouvernance cybersécurité et maîtrise des risques.

Objectifs

Approfondir les connaissances dans la gestion de la sécurité des systèmes d'information.

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 les traces informatiques.
- Système de détection d'intrusion.

Enjeux stratégiques de la cybersécurité

RÉFÉRENCE ***18***

DURÉE

3 jours

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.

Thématiques

Gouvernance et enjeux du cyberespace ; répondre à l'adversité dans le cyber ; organisation nationale et internationale.

Présentation

Le cyberespace, en tant que milieu transverse à de très nombreuses activités et politiques publiques, doit être compris dans son ensemble. Cette formation aborde donc ces enjeux du point de vue des activités qui ont lieu dans le cyberespace et l'adversité qu'on y rencontre, du point de vue national comme international. Elle est une aide à la décision pour ceux ayant à prendre en compte les enjeux actuels cyber.

Objectifs

Faire prendre conscience des enjeux du cyberespace (enjeux techniques, sociétaux et économiques).

Présenter l'adversité existant dans le cyber, ses objectifs et motivations et la façon de l'aborder.

Présenter l'organisation publique et les enjeux de gouvernant, au niveau national ou international face aux grandes puissances cyber.

Programme

- Présentation du cyberespace : ses caractéristiques, ses acteurs stratégiques, sa gouvernance décentralisée, avec les enjeux de pouvoirs internationaux.
- État de la menace d'origine cyber : attaquants, motivations, tendances, finalités, modes opératoires actuels.
- 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 : analyse de grandes puissances cyber, sécurité collective et stabilité du cyberespace, coopérations, alliances, rôle des organisations internationales (UE, ONU, OTAN, etc.).

Sécurité des systèmes industriels

RÉFÉRENCE ***19***

DURÉE

4 jours

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).

Thématiques

Introduction aux systèmes industriels ; sécurité des systèmes industriels ; projet de sécurisation d'un système industriel.

Présentation

À l'issue de la formation, le stagiaire sera capable de :

- réaliser un projet de mise en œuvre d'automates industriels et de sécuriser ce dernier ;
- identifier les menaces qui pèsent sur les systèmes industriels ;
- étudier et réaliser une architecture sécurisée d'un système industriel.

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

1er jour

Introduction aux systèmes industriels et programmation d'un automate industriel.

2ème jour

La cybersécurité des systèmes industriels et travaux pratiques.

3ème jour

Projet de sécurisation d'un système industriel.

4ème jour

Sécurisation périmétrique d'un système industriel (Pare-feu et commutateurs industriels).

Cloud Computing et DevOps : enjeux de sécurité

RÉFÉRENCE ***20***

DURÉE

2 jours

NIVEAU

Perfectionnement

Public

Architectes, personnels techniques, développeurs/DevOps, administrateurs, RSSI, Product Owner.

Prérequis

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

Principe d'usage d'un Cloud.

Guide d'hygiène informatique 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.

Avoir suivi le stage 26 (Sécurité des architectures virtualisées).

Thématiques

Enjeux techniques de sécurité du Cloud computing ; l'architecture technique d'un Cloud ; la sécurité des chaînes de développement automatisées.

Présentation

Vous souhaitez appréhender les problématiques de sécurité en environnement Cloud et DevOps.

Vous souhaitez comprendre le Cloud Computing et le DevOps, ses enjeux, ses risques et les bonnes pratiques de sécurisation.

Cette formation vous apportera la posture technique et stratégique de l'ANSSI.

Objectifs

- Comprendre les risques et les enjeux relatifs à l'usage du Cloud et des pratiques DevOps.
- Se familiariser avec SecNumCloud.
- Comprendre les recommandations de l'ANSSI relatives au Cloud et des pratiques DevOps.

Programme

- Cloud et SecNumCloud.
- Architecture d'un Cloud.
- Sécurité des API d'un Cloud.
- Orchestration dans le Cloud.
- Les spécificités de l'administration dans le Cloud.
- Pattern d'architecture.
- DevOps.

Administration sécurisée Windows

RÉFÉRENCE ***21***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Perfectionnement

Public

Ce stage s'adresse principalement aux administrateurs système, mais également aux administrateurs réseau et aux architectes.

Prérequis

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

Thématiques

Sécurité du réseau ; sécurité du système ; administration sécurisée ; journalisation.

Présentation

Présenter les bonnes méthodes d'administration ainsi que les fonctionnalités et les technologies permettant la gestion sécurisée d'un parc Windows. L'objectif principal est de reconnaître les méthodes mettant à risque des secrets d'authentification ou permettant un accès illégitime à un système d'information. Pour cela, le principe de défense en profondeur guide toute la formation.

Objectifs

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

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

Proposer une solution simple de journalisation.

Programme

- Principes de la défense en profondeur développés en détaillant les mécanismes qui peuvent être mis en place aux différents niveaux.
- Le réseau (accès, segmentation, sécurisation, supervision).
- Poste de travail (phase de démarrage, chiffrement de données, la sécurité de base, supervision).
- Comptes utilisateurs (jeton d'accès, comptes de service, comptes locaux, cycle de vie), authentification (LM/NTLM/Kerberos, les attaques et le multifacteur).
- Mots de passe (robustesse, verrouillage, stockage).
- Administrateurs (séparation par périmètre ; délégation, administration en tiers et bonnes pratiques), poste de travail (poste dédié, durci et leur gestion).
- Réseau d'administration (réseau distinct, serveurs de rebonds).
- Journalisation (centralisation d'événements, choix des événements, sysmon).

Sécurité physique et logique des composants

RÉFÉRENCE ***23***

DURÉE

5 jours
Présentiel (TP)

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 implémentation embarquée et/ou cryptographie.

Avoir suivi les stages 10 (Cryptographie) et 25 (Sécurité des systèmes embarqués) peut être un plus, mais n'est pas obligatoire.

Thématiques

Panorama des menaces sur les composants du logiciel au matériel ; attaques par observation et par injection de faute ; protection et évaluation des composants.

Présentation

Comprendre les notions de sécurité autour du composant et de 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.
- Sécurité du boot.
- Canaux auxiliaires et développement sécurisé.
- Attaques par injection de fautes.
- Attaques par cache.
- Mise en œuvre pratique des attaques.
- Attaques invasives.
- Certification des composants.

Analyse de code d'exploitation

RÉFÉRENCE ***24***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Expert

Public

Ingénieurs en investigation numérique, auditeurs SSI, analystes de code malveillant, analystes SOC.

Prérequis

Rétro-ingénierie x86-x64

Outils de débogage

Mode opératoire des attaquants

Thématiques

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

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

Présentation

Cette formation a pour objectif de présenter des techniques 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 d'exploitation.

Programme

- Mode opératoire des attaquants.
- ASM x86-x64.
- Exploitation d'un buffer overflow sous Linux.
- GDB/Windbg.
- Shellcode.
- Présentation des protections.
- Technique de contournement des protections.
- Architecture système.
- Architecture d'un navigateur web.
- Exploitation d'un navigateur.

Sécurité des systèmes embarqués

RÉFÉRENCE ***25***

DURÉE

3 jours

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.

Thématiques

Éléments d'architecture des systèmes embarqués ; démarrage sécurisé ; attaques par accès physique.

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.

Ces menaces pouvant remettre en cause toutes les mesures de sécurité en œuvre sur la couche applicative, il peut être nécessaire de considérer la problématique de la confiance au niveau du système embarqué.

Les équipements concernés par ce modèle de menace peuvent être tout type de système embarqué, objet connecté (IoT), appareil électronique pouvant être volé, perdu, ou opéré dans des conditions où la sécurité physique n'est pas assurée.

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

- Éléments 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.
- Chaîne de démarrage sécurisée : panorama des méthodes de sécurisation du démarrage, sur SoC et CPU
- Évolution de la sécurité : études 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.

Sécurité des architectures virtualisées

RÉFÉRENCE ***26***

DURÉE

3 jours

NIVEAU

Perfectionnement

Public

Architectes sécurité, responsables sécurité, administrateurs.

Prérequis

Aucun prérequis.

Thématiques

Technologies de virtualisation ; architectures virtualisées ; risques et bonnes pratiques liés à la virtualisation.

Présentation

Cette formation vise à présenter les enjeux de sécurité et à promouvoir les bonnes pratiques liées 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 les 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 type 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.
- Études de cas.

Sécurité firmware et chaîne de démarrage

RÉFÉRENCE ***27***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Expert

Public

DSI, RSSI, Ingénieurs.

Prérequis

Architecture d'un ordinateur (CPU, bus de communication, périphérique) ; principes de fonctionnement d'un programme binaire : chargement en mémoire, exécution.

Thématiques

Fonctionnement de la chaîne de démarrage x86/amd64 ; mécanismes d'intégrité et de confidentialité ; mise à jour et chaîne d'approvisionnement (supply-chain).

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.

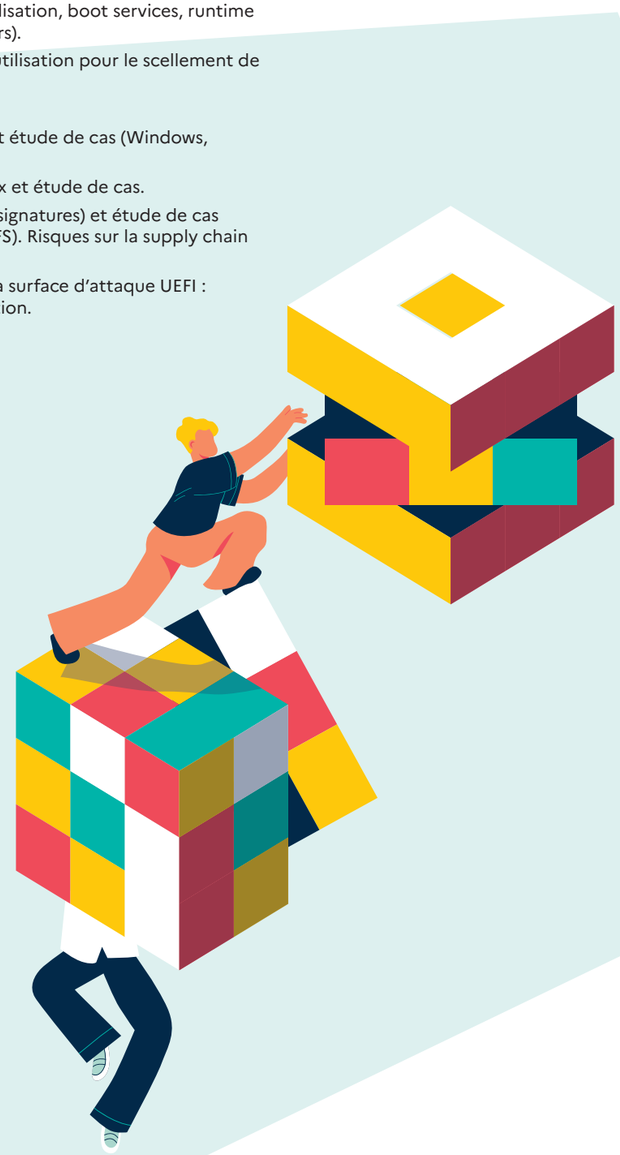
Les bonnes pratiques pour s'assurer du maintien d'un système en condition de sécurité.

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

- Éléments de la chaîne 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.
- 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.



Gestion de crise (Volet opérationnel, Stratégique, Communication)

RÉFÉRENCE ***29***

DURÉE

3 jours

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, responsables de la sécurité des systèmes d'information.

Prérequis

Sensibilisation aux enjeux cyber et/ou aux enjeux de gestion des crises.

Thématiques

Préparation à la gestion de crise cyber et entraînement ; opérations de crise d'origine cyber et pilotage de crise ; communication de crise.

Présentation

Cette formation a pour objectif de former les acteurs à la gestion de crise d'origine cyber notamment via des mises en situation (scénario « fil rouge » suivi tout au long de la formation).

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).

Sécurité firmware et chaîne de démarrage

Programme

1er jour

- Préparation aux crises cyber (construire son dispositif de crise).
- Planification gouvernementale et gestion de crise d'origine cyber de l'État.
- S'entraîner à gérer une crise cyber.
- Activer son dispositif de crise et premières actions à mener.
- Pilotage de crise et points de situation.

2ème jour

- Opérations de crise d'origine cyber.
- Anticipation dans la crise.
- Continuité d'activité.
- Sortir et capitaliser sur une crise (avec grand témoignage).

3ème jour

- Communication de crise.
- Exercice : simulation d'une gestion de crise cyber (niveau stratégique).

Analyste SOC

RÉFÉRENCE ***30***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Perfectionnement

Public

La formation se destine aux analystes SOC exploitant les alertes ou produisant de nouvelles alertes, soit nouvellement arrivés dans un SOC soit déjà présents.

Prérequis

La formation ne nécessite pas d'autres formations présente au catalogue du CFSSI.

Thématiques

Méthodologies du SOC et de l'analyste SOC ; méthodes de détection sous Windows ; méthodes de détection pour les autres plateformes.

Présentation

La formation a pour objectifs 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

Les apprenants doivent pouvoir reconnaître une attaque connue sous Windows, caractériser cette attaque. Ils doivent également 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.
- Quoi collecter ?
- 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 opérationnelle.

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 : ActiveDirectory, Kerberos, NTLM, lsass, ntds, sam.
- Moyens de détection des outils et techniques de vol d'authentifiant dont mimikatz.
- Techniques d'attaque et de détection Powershell.
- Prérequis et création de règles Sysmon.
- Détection des techniques de latéralisation : RDP, SMB, PSRemoting, WMI.
- Détection de la persistance : création de services, tâches planifiées, clés de registres, dossiers startup.
- Repérage des traces générées par les outils communément utilisés par les attaquants : Cobalt Strike, Empire, Lolbins.
- Fonctionnement et détection des élévations de privilège : SID, Niveau d'intégrité, token.
- Détection en amont de la reconnaissance faite par l'attaquant au sein du SI : adfind, bloodhoud, LOLBins.

Techniques de détection de compromission d'autres environnements :

- Linux.
- Réseau : scans, flux, beaconning, trafic HTTP/HTTPS sortant, trafic DNS.

Processus métier des analystes :

- Processus d'investigation d'une alerte.
- Processus de chasse (hunting).

Nouveau

Réseau & Sécurité

*RÉFÉRENCE **31***

DURÉE

5 jours
Présentiel (TP)

NIVEAU

Expert

Public

Auditeurs, Pentesteurs, Administrateurs Réseau.

Prérequis

Réseaux.

Thématiques

Réseau ; sécurité ; cryptographie.

Présentation

Cette formation propose un approfondissement des mécanismes et des protocoles réseau, ainsi que les attaques classiques et contre-mesures qui peuvent exister. Elle propose une alternance entre contenu théorique et manipulations, au cours desquels les apprenants réaliseront des configurations réseau, forgeront et enverront des paquets (pour réaliser des attaques ou pour scanner), analyseront des réponses, et mettront en œuvre des durcissements. Une partie du cours traitera également des cœurs de réseaux d'opérateurs de télécommunication.

Objectifs

Approfondir les connaissances théoriques en réseau et la compréhension des mécanismes réseau, manipuler des paquets, comprendre et mettre en œuvre des attaques classiques et des contre-mesures.

Programme

1er jour

Couche 2 et mécanismes associés. Ethernet, ARP, VLAN. Ecriture d'un scanneur ARP, écriture d'un outil pour faire de l'ARP spoofing.

2ème jour

Couche 3 et mécanismes associés. IPv4, routage, DHCP, DHCP Snooping.

3ème jour

Couche 4 et + : TCP, UDP. TLS, Quic.

4ème jour

Scan : méthodes et outils. Ecriture d'un SYN-scanneur. Wifi : WEP, WPA, WPA2, WPA3 : attaques et état de l'art. Capture et analyse des trames de management, fingerprinting.

5ème jour

Réseaux d'opérateurs. BGP. ORPF.

Nouveau

Analyses statiques et dynamiques des architectures matérielles et logicielles

*RÉFÉRENCE **32***

DURÉE

3 jours
Présentiel (TP)

NIVEAU

Expert

Public

R&D Cybersécurité matérielle et logicielle.

Prérequis

Aucun prérequis.

Thématiques

Architectures matérielles et logicielles ; protocole de communication entre composants (UART, SPI, I2C).

Présentation

Analyser le logiciel embarqué dans le matériel (ou firmware) est souvent perçu comme une tâche ardue. Après une introduction présentant les principales architectures matérielles et les interfaces majeures de communication entre composants (UART, SPI, I2C etc.), ce stage présente un état de l'art des techniques statiques et dynamiques de rétro-ingénierie matérielle. Des travaux pratiques illustreront les méthodes d'extraction de mémoire, d'écoute de bus ainsi que l'utilisation des outils de désassemblage permettant l'analyse des micro-logiciels extraits.

Objectifs

Apprendre les bases du fonctionnement des protocoles usuels et du mécanisme des infrastructures de débogages.

Programme

Après une journée théorique de présentation des protocoles usuels UART (et USART), I2C et SPI, les stagiaires prendront en main une plateforme matérielle sur laquelle ils implémenteront un master SPI en « bit bang » c'est-à-dire en utilisant uniquement des GPIOs.

Le stage consistera ensuite en la prise en main d'outils de communications SPI sur étagère. Ensuite une présentation rapide du protocole de communication employé par la puce flash SPI sera faite et des opérations d'extraction de firmware seront effectuées sur des exemples pratiques. La formation continuera en adoptant une démarche similaire vis à vis des mémoires I2C. La formation se terminera en évoquant le protocole UART qui est un protocole incontournable dans l'embarqué. Une illustration des outils permettant l'analyse des dump mémoires sera proposée.

Nouveau

Enjeux de sécurité DevOps dans la gestion de configuration et de déploiement dans les SI

RÉFÉRENCE ***33***

DURÉE

4 jours
Présentiel (TP)

NIVEAU

Expert

Public

Ingénieurs DevOps, administrateurs systèmes et réseaux, RSSI.

Prérequis

Les prérequis suivants sont attendus :

- Administration de systèmes Linux.
- Langage de scripting (bash, python et/ou ruby).
- Gestion de versionning de code avec git.
- Connaissance de base en réseau.

Thématiques

Gestion de configuration automatique avec Puppet et Ansible ; déploiement continu de systèmes d'information en environnement Linux ; enjeux de sécurité pour les ingénieurs DevOps.

Présentation

L'un des défis majeurs pour les administrateurs de SI consiste à mettre en œuvre une stratégie sécurisée et continue rythmant le déploiement et l'audit des systèmes et des services qui composent l'infrastructure administrée. Dans ce contexte, il est nécessaire de disposer d'outils automatisés de déploiement, d'orchestration et de gestion de configurations systèmes comme Puppet ou Ansible. Cette formation présente ces deux outils et offre un ensemble de TP illustrant les bonnes pratiques à mettre en œuvre dans leur utilisation dans le cadre du déploiement d'un SI complet en environnement Linux.

Objectifs

Connaître les caractéristiques et le fonctionnement des outils de configuration automatiques comme Puppet ou Ansible.

Comprendre comment optimiser le pilotage d'un parc de serveurs Linux et le déploiement de services associés.

Maîtriser les bonnes pratiques CI/CD (Continuous Integration / Continuous Distribution) et IaC (Infrastructure as Code).

Programme

Après une première journée présentant les enjeux de sécurité liés aux développements DevOps de type Insfrastructure as Code (IaC), ainsi que les principaux outils de gestion de configuration automatique (comme cfengine, chef, puppet, saltstack, ansible ou encore terraform), les stagiaires prendront en main lors des journées suivantes les deux principales solutions utilisées actuellement sur le marché pour ce type d'intégration que sont puppet et ansible. L'architecture et le fonctionnement général de ces technologies seront présentés pour mieux cerner les points communs et les différences entre chaque approche, et des exemples pratiques seront proposés pour illustrer leur bonne utilisation au quotidien dans le cadre d'un déploiement effectif d'une infrastructure de SI fonctionnelle en environnement Linux incluant les principaux services attendus.

Nouveau

Sécurité des systèmes Linux

RÉFÉRENCE ***34***

DURÉE

4 jours
Présentiel (TP)

NIVEAU

Expert

Public

Ingénieurs, administrateurs systèmes, architectes.

Prérequis

Le stage 27 (Sécurité firmware et chaîne de démarrage) n'est pas un prérequis mais permet d'aborder la problématique de l'intégrité au démarrage d'un système Linux sur une plateforme x86.

Thématiques

Durcissement du noyau Linux ; durcissement de l'espace utilisateur Linux ; réduction de surface d'attaque (noyau et espace utilisateur).

Présentation

L'environnement Linux, son noyau comme son espace utilisateur, que ce soit pour un serveur, un PC ou en embarqué est un environnement riche et complexe. De nombreux facteurs sont à prendre en compte lors du durcissement de ce dernier. Le but de ce stage est de couvrir un maximum des notions de durcissement et d'applications du principe de défense en profondeur à ce système afin d'augmenter la sécurité de ce dernier. Un ensemble de travaux pratiques permettent de tester sur des exemples concrets les concepts présentés.

Objectifs

Comprendre les mécanismes de durcissement d'un système Linux, son noyau et son espace utilisateur.

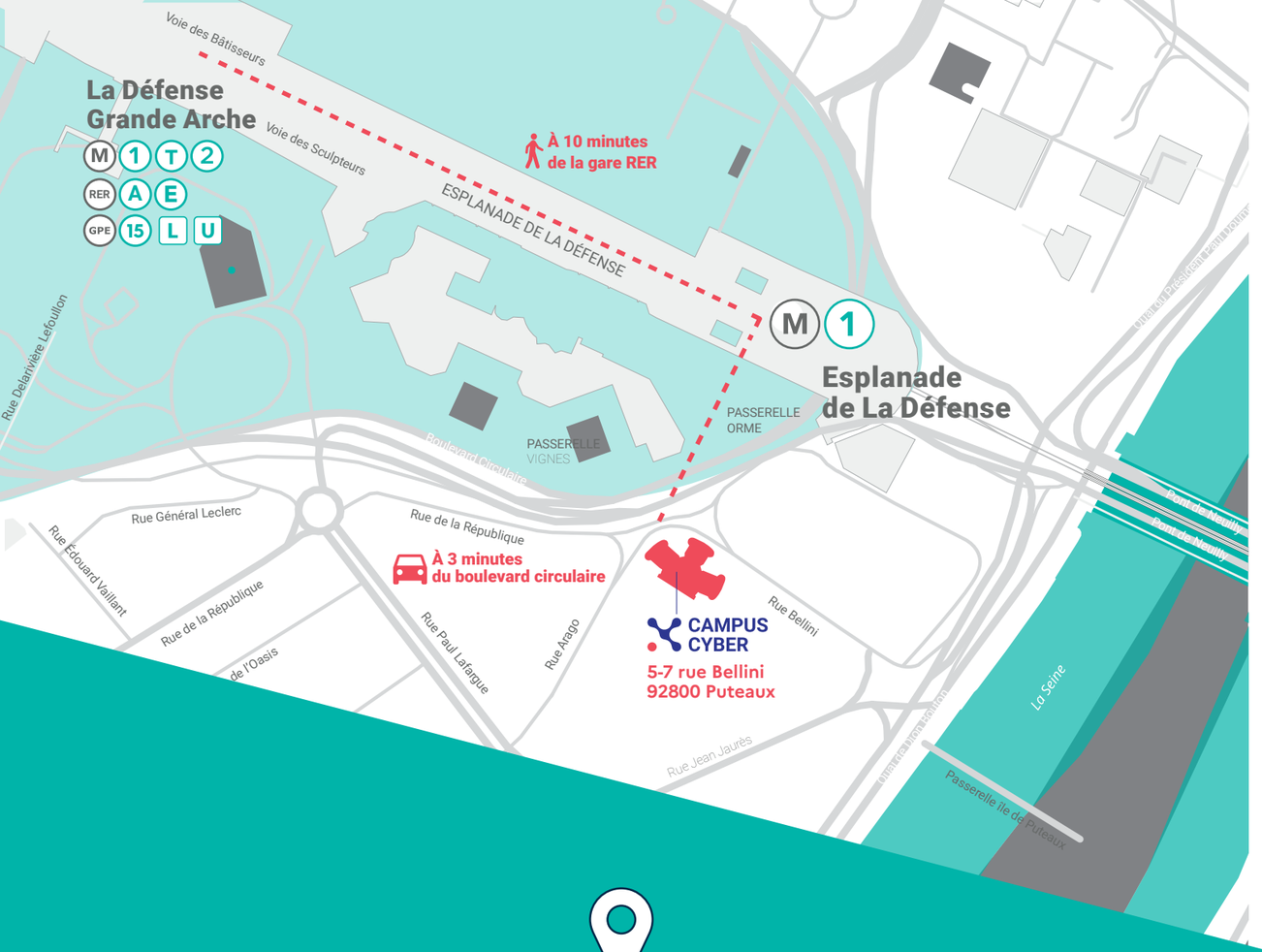
Programme

Noyau :

- Présentation de l'environnement (implémentation des mécanismes d'isolation dans le noyau).
- TP durcissement du noyau.

Espace utilisateur :

- Présentation de l'environnement (application des mécanismes d'isolation offerts par le noyau à l'espace utilisateur).
- TP durcissement de l'espace utilisateur (authentification, séparation et application du principe de moindre privilège).



Accès

Transport le plus proche

M 1
Esplanade de la Défense

RER A
La Défense (Grande Arche)

Accessibilité routière

Quai de Dion Bouton
à 200 mètres

Boulevard circulaire au pied
de l'immeuble

CFSSI - ANSSI, Campus Cyber
5-7 rue Bellini - 92800 Puteaux - cfssi@cfssi.gouv.fr

Pour plus d'informations :

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

ANSSI

51, boulevard de la Tour Maubourg
75700 PARIS 07 SP
www.ssi.gouv.fr - communication@ssi.gouv.fr

Version 1.0 – Juin 2023