



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Catalogue
du centre
de formation
à la sécurité
des systèmes
d'information
2025-2026



**Catalogue
du centre
de formation
à la sécurité
des systèmes
d'information**
2025-2026







Sommaire

Présentation du centre de formation 6

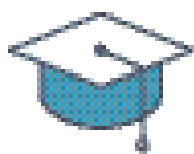
Formations	6
Fonctionnement des formations	8

Fiches de formations 10

Premiers pas en TEMPEST	11
Sécurité électromagnétique (TEMPEST)	12
Certificats électroniques	14
Audit technique en sécurité des systèmes d'information	16
Sécurité des applications Web	17
Cryptographie	19
Sécurité des réseaux sans fils	20
Homologation Sécurité	21
Incidents de sécurité	22
Intégrer la sécurité numérique dans les projets SI de l'État	23
Enjeux stratégiques de la cybersécurité	24
Sécurité des systèmes industriels	25
Cloud Computing et DevOps : enjeux de sécurité	26
Administration sécurisée Windows	27
Sécurité physique et logique des composants	28
Analyse de code d'exploitation	29
Sécurité des systèmes embarqués	30
Sécurité des architectures virtualisées	31
Sécurité Firmware et de la chaîne de démarrage	32
Rétroconception	34
Gestion de crise (Volet opérationnel, Stratégique, Communication)	35
Analyste SOC	37
Réseau & Sécurité	39
Analyses statiques et dynamiques des architectures matérielles et logicielles	40
Administration Systèmes Linux et stratégies Devops dans la gestion de config. et le déploiement de SI... ..	41
Sécurité des systèmes Linux avancée	43
Cryptographie post-quantique	44
Pilotage de la remédiation	46

NOUVEAU

Sensibilisation aux enjeux de cybersécurité de l'Intelligence Artificielle (Date à définir - à compter du second semestre 2026)	47
---	----



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.cyber.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.cyber.gouv.fr/administration/formations/titre-essi/

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

3

Le MOOC SecNumacadémie

Dans le cadre de sa mission de sensibilisation, l'ANSSI propose SecNumacadémie 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 SecNumedu

Le label SecNumedu 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.



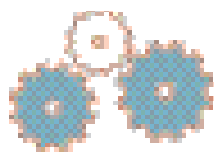
Plus d'informations : www.cyber.gouv.fr/entreprise/formations/secnumedu/

5

La labellisation SecNumedu 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**.

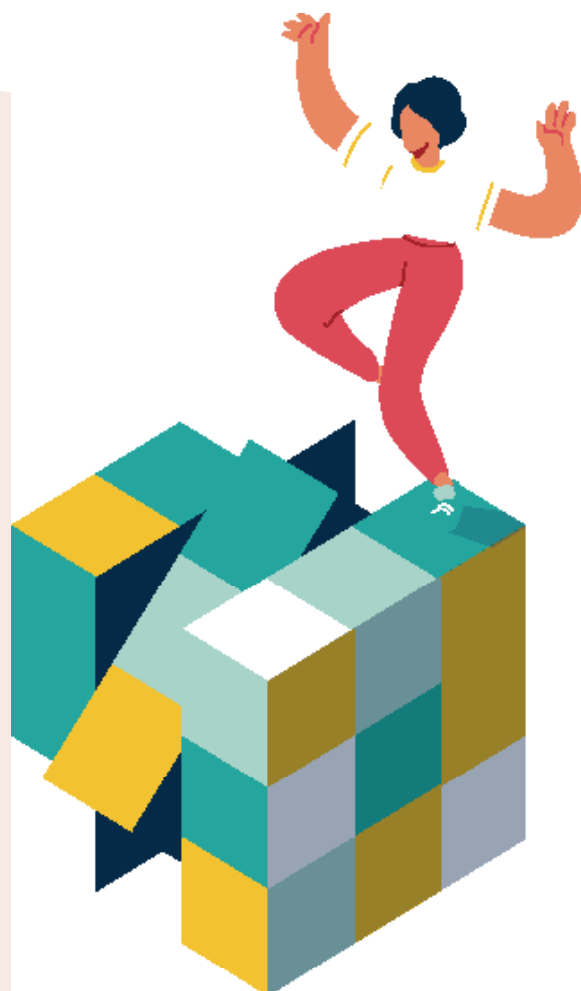
Les organismes de formation qui proposent la formation labellisée **s'engagent sur une charte**. La formation est inscrite au Répertoire Spécifique de France Compétences et/ou la formation se déclare conforme à un cahier des charges reconnu par l'ANSSI.



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 1^{er} jour

L'accueil du 1^{er} 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.



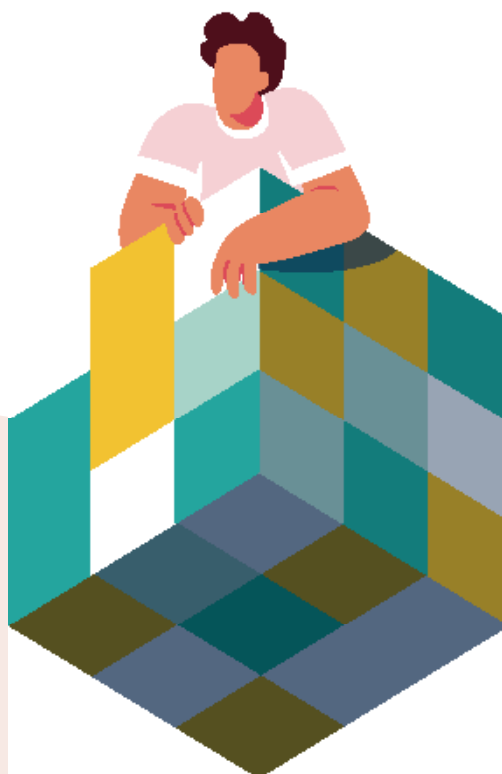
Restauration et pause-café (8h-17h)

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

2

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.

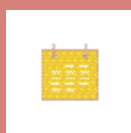




Fiches de
formation

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

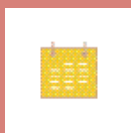
Sensibiliser les participants à la menace liée aux ondes électromagnétiques sur les systèmes d'information classifiés ou sensibles dans leur environnement quotidien.

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. Le stage 2a n'est en aucun cas un prérequis du stage 2.

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.

Sécurité électromagnétique (TEMPEST)

Programme

1^{er} jour

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

2^{ème} jour

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

3^{ème} jour

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

4^{ème} jour

- Cage de FARADAY Théorie.
- Ateliers pratiques.

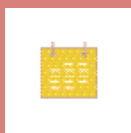
5^{ème} jour

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



Certificats électroniques

RÉFÉRENCE 6



DURÉE

**2,5 jours
Présentiel (TP)**

NIVEAU

Initiation

Public

Personnes 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.

Les apprenants ciblés 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 réglementaire :

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

Référentiel documentaire d'une IGC :

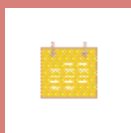
- Savoir ce qu'est une politique de certification et son contenu.
- Les conditions générales d'utilisation d'un service de signature électronique.
- Les autres documents qui doivent être publiés tel que les certificats d'AC, les listes de révocations, les répondeurs OCSP.
- Les documents à accès restreint 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.

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

Aucun prérequis. Le stage est accessible uniquement après avoir complété un questionnaire qui sera soumis à la validation préalable de l'intervenant.

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.

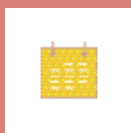
Programme

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

Sécurité des applications Web

Pas de session au 2nd semestre 2026 - Stage en cours de refonte

RÉFÉRENCE 9



DURÉE

3,5 jours



NIVEAU

Perfectionnement

Public

Ce stage s'adresse aux développeurs d'applications web.

Prérequis

Cette formation ne requiert pas d'avoir suivi une autre formation du CFSSI. En revanche, 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

La formation se déroule sur cinq jours composés de dix demi-journées thématiques décrites dans le programme ci-après.

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

1^{er} 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.

2^{ème} 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.

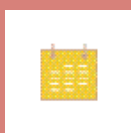
3^{ème} jour

- **Authentification et gestion des sessions** : mécanismes d'authentification répandus sur le web, authentification multifacteur, maintien de session 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.

4^{ème} jour matinée seulement

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

Cryptographie



DURÉE

19 jours



NIVEAU

Expert

RÉFÉRENCE 10

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 fondées sur la cryptographie.

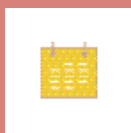
Aider à comprendre la nature des menaces, les raisonnements cryptographiques, et la justification des pratiques et des règles.

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 :

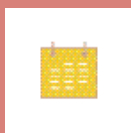
- les technologies sans-fil et les architectures associées ;
- les risques relatifs à l'usage de réseau sans fil ;
- les contre-mesures disponibles et leurs limites.

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

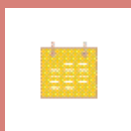
- Savoir bâtir et conduire un processus d'homologation.
- Savoir constituer un dossier d'homologation.
- Savoir motiver la prise de décision d'homologation.
- Comprendre la démarche d'homologation et son inscription dans le cadre réglementaire.

Programme

- Objectif de la démarche d'homologation.
- 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. Le stage est accessible uniquement après avoir complété un questionnaire qui sera soumis à la validation préalable de l'intervenant.

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

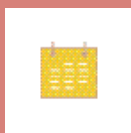
Être capable d'appréhender les différentes phases du traitement d'incidents de sécurité en ayant les bons réflexes et en utilisant des outils adaptés, notamment lors de la qualification/analyse d'un système compromis.

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 direction 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.

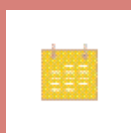
Cadrer et adapter la démarche de maîtrise du risque cyber au contexte et à la criticité du SI, en lien avec la réglementation, et particulièrement dans le cadre d'une démarche d'homologation.

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.

Enjeux stratégiques de la cybersécurité



DURÉE

3 jours



NIVEAU

Initiation

RÉFÉRENCE 18

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 cyberspace ; répondre à l'adversité dans le cyber ; organisation nationale et internationale.

Présentation

Le cyberspace, 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 cyberspace 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 cyberspace (enjeux techniques, sociétaux et économiques).

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

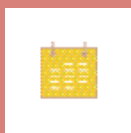
Présenter l'organisation publique et les enjeux de gouvernant, au niveau national ou international face aux grandes puissances cyber.

Programme

- Présentation du cyberspace : 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 cyberspace, 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 stage - 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

1^{er} jour

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

2^{ème} jour

La cybersécurité des systèmes industriels et travaux pratiques.

3^{ème} jour

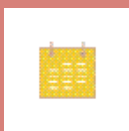
Projet de sécurisation d'un système industriel.

4^{ème} 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.

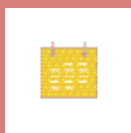
Programme

- 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

Stage suspendu à compter du 1er janvier 2026

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

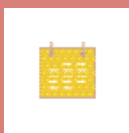
Présenter aux administrateurs les pratiques à bannir et celles à privilégier.
Faire un panorama des fonctions et des outils qui permettent d'augmenter le niveau de sécurité d'un parc Windows.
Proposer une solution simple de journalisation.

Programme

- Principes de la défense en profondeur développés en détaillant les mécanismes qui peuvent être mis en place aux différents échelons.
- 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

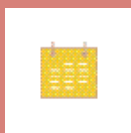
- Comprendre les menaces qui pèsent sur les implantations matérielles (cartes à puce, microcontrôleurs, systèmes embarqués, etc.).
- Suivre l'état de l'art sur les protections ou les contre-mesures existantes et connaître les outils permettant d'évaluer leur efficacité.
- Connaître les problématiques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

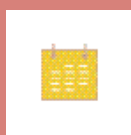
Objectifs

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



DURÉE

3 jours



NIVEAU

Expert

RÉFÉRENCE 25

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.

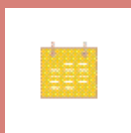
Programme

- 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

Pas de session au 2nd semestre, stage en cours de refonte

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

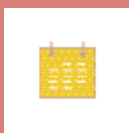
Connaître les technologies et les principes sous-jacents à la virtualisation.
Être sensibilisé aux risques et connaître les bonnes pratiques liées à la mise en œuvre de la virtualisation.
S'approprier une démarche de sécurisation des architectures virtualisées.

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(s) associé(s), 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.

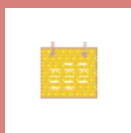
L'utilisation d'attestation distante dans le cadre d'une approche Zero Trust.

Programme

- Éléments de la chaîne de démarrage : pre-boot, UEFI, bootloader, OS.
- Pre-boot : Intel BootGuard, AMD PSP.
- UEFI : structure(s) 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 études 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.

Rétroconception

RÉFÉRENCE 28



DURÉE

5 jours
Présentiel (TP)



NIVEAU

Expert

Public

Cette formation s'adresse aux personnes ayant une base solide en informatique (expert en système ou programmation) et souhaitant s'initier à la rétro-conception.

Prérequis

Avoir des notions de programmation bas-niveau (C par exemple) et maîtriser un langage de scripting (Python).

Les stagiaires doivent OBLIGATOIREMENT, pour suivre cette formation, apporter un ordinateur portable et posséder une licence IDA pro pour Windows avec le décompilateur Hexrays x86-64.

Thématiques

Rétro-conception, assembleur, décompilation

Présentation

Cette formation apporte les bases nécessaires pour la rétroconception de programmes exécutables. Après une introduction à l'assembleur (x86-64), elle apportera les bases pour apprendre à faire de la rétro-conception sur le logiciel IDA de programmes pour Windows.

Objectifs

Avoir des bases en analyse et rétro-conception de programmes compilés. Cette formation apporte un premier socle permettant de se familiariser avec les langages assembleurs ainsi que les outils utilisés pour la rétro-conception.

Programme

- Fonctionnement d'un CPU, instructions x86-64,
- Lecture / écriture d'assembleur,
- Compilation / Décompilation,
- Spécificités Windows : Format PE, API windows,
- Debugger / tracer un programme,
- Désobfuscation, scripting.

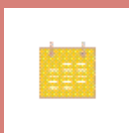
Tout au long des cours, des TPs apporteront une mise en pratique sur IDA, où les concepts suivants, entre autres, sont introduits :

- Structures / énumérations
- Travailler sur la vue décompilée
- Renommage / cast de variables / fonctions

La formation se terminera sur une journée entière de TP

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).

Gestion de crise (Volet opérationnel, Stratégique, Communication)

Programme

1^{er} 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.

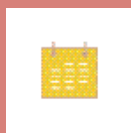
2^{ème} jour

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

3^{ème} jour

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

Analyste SOC



DURÉE

5 jours
Présentiel (TP)



NIVEAU

Perfectionnement

RÉFÉRENCE 30

Public

La formation est destinée aux analystes SOC qui exploitent des alertes ou produisent des règles de détection. Elle est adaptée à des analystes SOC prenant leurs fonctions ou déjà en poste.

Prérequis

Le stage est accessible uniquement après avoir complété un questionnaire qui sera soumis à la validation préalable de l'intervenant. La maîtrise des fondamentaux en système, réseau et sécurité informatique est nécessaire. Une première expérience sur un SIEM est bienvenue.

Thématiques

Méthodologies du SOC et de l'analyste SOC ; méthodes de détection sous Windows ; méthodes de détection réseau.

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 réalisées sous Windows ou sur le réseau. La méthodologie de travail consiste, pour chaque thème, à présenter la théorie puis la pratique de la démarche d'analyse et de qualification des journaux, pour préciser les contours de l'attaque. Ces analyses sont uniquement conduites à partir d'éléments à disposition d'un SOC (journaux, SIEM et NIDS).

Objectifs

Les apprenants doivent savoir analyser une alerte réseau ou Windows déclenchée par un SIEM et déterminer comment la traiter. Ils doivent également pouvoir produire des signatures sur les schémas connus, voire sur de nouvelles méthodologies d'attaques.

Programme

Panorama de la détection

- Présentation de la menace (Kill Chain, évolution de la menace)
- Identification du périmètre de supervision
- Identification des sources de données et présentation de la chaîne de collecte
- Centralisation des événements, normalisation, enrichissement, stockage
- Ingénierie de la détection et conception de règles (Pyramid of Pain, cycle de vie d'une règle, non-régression)
- Qualification et analyse d'alertes (RUN, biais cognitifs, triage des alertes, fatigue d'alertes, gestion des faux-positifs, outillage d'investigation)
- Présentation de cas pratiques

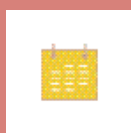
Techniques de détection pour Windows

- 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, Bloodhound, LOLBins.

Techniques de détection réseau

- Les caractéristiques de la détection réseau
- Comprendre le réseau pour détecter
- Evolution de la menace
- Les sources de données de détection réseau
- La détection basée sur les journaux d'applicatifs réseaux
- La détection basée sur l'analyse de trafic réseau
- Les techniques de détection réseaux
- Les actions des attaquants sur le réseau
- Détection de reconnaissance, découverte et collecte
- Détection d'exploitation
- Détection de canaux cachés et exfiltration

Réseau & Sécurité



DURÉE

5 jours
Présentiel (TP)



NIVEAU

Perfectionnement

RÉFÉRENCE 31

Public

Auditeurs, Pentesteurs, Administrateurs Réseau.

Prérequis

Etre à l'aise avec le terminal Linux, avoir déjà utilisé python (une simple introduction de quelques heures suffit)

Thématiques

Réseaux, sécurité, attaques réseau

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

1^{er} jour

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

2^{ème} jour

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

3^{ème} jour

IPv6, TCP, UDP

4^{ème} jour

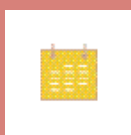
TLS, et protocoles applicatifs (SSH, SMB, etc.)

5^{ème} jour

Réseaux d'opérateurs. BGP. ORPF.

Analyses statiques et dynamiques des architectures matérielles et logicielles

RÉFÉRENCE 32



DURÉE

4 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

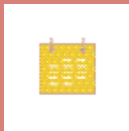
Apprendre les bases du fonctionnement des protocoles usuels et du mécanisme des infrastructures de débogages.

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.

Administration Systèmes Linux et stratégies DevOps dans la gestion de configuration et de déploiement de SI



DURÉE

**5 jours
Présentiel (TP)**



NIVEAU

Perfectionnement

RÉFÉRENCE 33

Public

Ingénieurs DevOps, administrateurs systèmes et réseaux, RSSI.

Prérequis

Eventuellement (mais non nécessaire) : Stage 20 et 26

En revanche, les prérequis suivants sont attendus :

- Administration de systèmes Linux.
- Fluidité dans l'utilisation de lignes de commandes shell,
- Langage de scripting (bash, python et/ou ruby).
- Gestion de versionning de code avec git.
- Connaissance de base en réseau.

ATTENTION: la plupart des supports présentés seront en anglais même si la formation se déroule en français.

Thématiques

Administration de systèmes Linux à large échelle

Stratégie DevOps, DevSecOps et outils/concepts associés

Outils de gestion de configuration (Puppet, Ansible, Terraform)

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 d'appréhender correctement les enjeux techniques et les mécanismes sous-jacents guidant l'administration des systèmes et de disposer d'outils automatisés de déploiement, d'orchestration et de gestion de configurations systèmes comme Puppet, Ansible ou Terraform. Cette formation, qui se concentre sur les systèmes Linux, vise à présenter de façon didactique l'architecture et l'administration de systèmes Linux, et de donner un ensemble d'outils et de bonnes pratiques permettant d'assurer l'administration de ce type de système de façon efficace, sécurisée et collaborative. L'accent est mis sur la pratique en proposant un très grand nombre de TP permettant de prendre en main et d'illustrer les concepts et outils présentés.

Objectifs

Comprendre les caractéristiques des systèmes Linux et des architectures matérielles et logicielles sous-jacentes.

Comprendre les outils et les bonnes pratiques permettant d'assurer l'administration et le pilotage d'un parc de serveurs Linux de façon efficace, sécurisée et collaborative

Maîtriser le fonctionnement et les bonnes pratiques à utiliser dans les outils de gestion de configuration automatiques (comme Puppet, Ansible ou Terraform)

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

Programme

La première journée est principalement orientée vers les aspects opérationnels (Ops) de l'administration de systèmes Linux

Computational System Architecture and Administration

- Introduction
- Computational System Architecture
- Example of a Computational System Architecture: the ULHPC Facility
- Important Elements of Linux System Administration
- Unix Shell Tips and Tricks
- Filesystem Hierarchy Standard
- Linux Boot Process
- Partitioning
- User Management
- Service Management
- Unified Virtualization Stack Management with libvirt
- LSM and MAC Policy enforcement
- DevOps

La seconde journée s'intéresse aux outils et concepts associés aux stratégies DevOps :

- **DevOps: preliminary tools and concepts**
- PGP / GPG: Gnu Privacy Guard
- Password Management
- Backup, backup, backup (and restore)
- **Distributed Version control with git**
- **SSH Secure SHell: Basic and Advanced Usage**

La troisième journée s'intéresse aux concepts de recherche reproductibles (appliqués à l'administration de système Linux) et introduit les concepts d'Infrastructure as Code (IaC) et de CI/CD (Continuous Integration Continuous Distribution) :

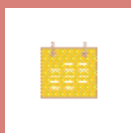
- **Reproducible Research and IT Management**
- Reproducible Research
- Sandboxed Environment for reproducible development (python, direnv, ruby, asdf, nix...)
- Reproducible Systems: Packer, mkosi
- Reproducible VMs: Vagrant,
- Reproducible Containers: Podman
- **IaC and CI/CD**

Les quatrième et cinquième journées sont dédiées aux principaux outils de gestion de configuration automatique (comme cfengine, chef, puppet, saltstack, ansible ou encore terraform). La formation se concentrera sur trois d'entre eux :

- **Configuration Management with Puppet**
- **Configuration Management with Ansible**
- **Configuration Management with Terraform**

Sécurité des systèmes Linux avancée

RÉFÉRENCE 34



DURÉE

5 jours
Présentiel (TP)



NIVEAU

Expert

Public

Administrateurs systèmes, auditeurs, architectes.

Prérequis

Connaissances approfondies de l'administration des systèmes Linux.
Être à l'aise avec la manipulation d'un système Linux via un terminal.

Il est indispensable que le stagiaire soit à l'aise avec les notions suivantes :

- Gestion des permissions de fichier Linux.
- Installer et mettre à jour un paquet.
- Éditer un fichier dans un terminal.
- Configurer un service systemd.
- Lire et écrire des règles de pare-feu iptables ou nftables.
- Utiliser SSH.

Thématiques

Configuration du noyau Linux, Cloisonnement des processus, Gestion des privilèges, Cloisonnement réseau

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

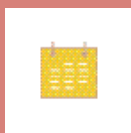
Le but est d'analyser et comprendre les mécanismes de durcissement et de cloisonnement du système Linux ainsi que leurs limites. Pour ce faire, les API de bas niveau sont présentées. Les outils de containerisation tel que Docker ou Podman ainsi que les outils de sandbox comme Firejail ou bubblewrap concus par dessus ces mécanismes ne seront pas présentés.

Programme

- Architecture du système.
- Configuration du noyau Linux.
- Authentification et identités.
- Contrôle d'accès discrétionnaire (DAC)
- Contrôle d'accès obligatoire (MAC)
- SELinux, AppArmor, ...
- Mécanismes d'élévation et délégation de privilèges.
- Capabilities, polkit, ...
- Mécanismes de cloisonnement.
- Namespaces, Cgroups, seccomp, ...
- Durcissement de service systemd.
- Isolation réseau.
- Interfaces virtuelles, pare-feu, ...

Cryptographie Post-Quantique (État de la menace, enjeux et actions)

RÉFÉRENCE 35



DURÉE

**1 jour
Présentiel**

NIVEAU

Initiation

Public

Cette formation d'adresse à un public non familier du domaine de la cryptographie qui souhaiterait un aperçu général de la menace et des enjeux (décideurs, développeurs, managers d'équipes R&D...)

Prérequis

Aucun prérequis

Les stagiaires doivent OBLIGATOIREMENT apporter un ordinateur portable.

Thématiques

Menace quantique, cryptographie post-quantique, recommandations

Présentation

Elle présente les grandes lignes de l'état de la menace quantique, les enjeux industriels et techniques de prise en compte de cette menace ainsi que la réaction du monde académique et des entités étatiques internationales.

Objectifs

- Comprendre et relativiser la menace quantique,
- Savoir interagir avec des experts en calcul quantique et cryptographie post-quantique,
- Connaître l'actualité internationale et la position française sur le sujet.

Programme

Pendant la matinée, les 3 points suivants seront abordés :

- Présenter l'algorithme de Shor sur des exemples. Il s'agit de l'algorithme à l'origine de la menace quantique. L'important est de comprendre l'aspect novateur et le gain en temps de calcul que cet algorithme permettrait,
- Eclaircir l'état de la recherche en technologies quantiques. Quelle est la différence entre l'échange de clés quantique, la «suprématie quantique» ou encore les ordinateurs quantiques universels ? L'idée est d'aborder factuellement l'état de la recherche en informatique quantique en confrontant les différentes visions et en évitant l'écueil des «effets d'annonce»,
- Etablir l'état de la menace sur nos systèmes et les potentielles actions à mener. Quels systèmes seraient vulnérables à la menace quantique ? Qu'est-ce que la cryptographie post-quantique ? Nous allons présenter l'actualité internationale en termes de recherche et les différentes recommandations étatiques,

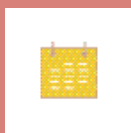
Cette partie sera conclue par un quizz interactif non technique pour consolider les acquis.

L'après-midi est consacrée à l'approfondissement individuel ou en petit groupe d'un aspect lié au cours de la matinée (approfondissement de l'algorithme de Shor, analyse du risque quantique, confrontation des positions étatiques internationales, enjeu des brevets en cryptographie post-quantique...).

Plusieurs supports (vidéos, corpus documentaires, sites internet, codes) ainsi qu'un guide avec questions précises sera proposé. Une fois les études terminées, une mise en commun est prévue avec l'ensemble du groupe. L'après-midi se terminera avec plusieurs études de cas concrets et des discussions ouvertes.

Pilotage de la Remédiation

RÉFÉRENCE 36



DURÉE

2 jours
Présentiel (TP)



NIVEAU

Expert

Public

RSSI, DSI, Chef de projet SSI
Toute personne amenée à piloter une remédiation d'incident SSI

Prérequis

- Connaissance des concepts d'architecture des systèmes d'informations
- Connaissance des concepts d'EBIOS RM

Thématiques

- Principes de remédiation à une cyberattaque
- Référentiel « E3R » : Endiguement, Eviction, Eradication et Reconstruction
- Gestion du plan de remédiation

Présentation

Former à la gestion de la remédiation d'un incident de sécurité informatique avec la séquence « E3R » (Endiguement, Eviction, Eradication et Reconstruction) et les 3 plans types.

Elle explicite la mise en œuvre pratique du pilotage de la remédiation dont le cadre conceptuel est défini dans le guide opérationnel «Piloter la remédiation» du corpus documentaire «Cyberattaques et remédiation» publié sur le site de l'ANSSI.

Objectifs

- Piloter la remédiation avec la séquence « E3R » et les 3 plans types
- Elaborer et exécuter un plan de remédiation

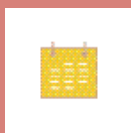
Programme

- Etat des lieux de la remédiation
- Terminologie de la remédiation
- Les principes d'élaboration d'un plan de remédiation
- Exécution de la remédiation
- Construire un plan de remédiation
- Anticiper/Préparer la remédiation
- Exercice sur table
- Retourner vers un état normal du SI

Nouveau

Sensibilisation aux enjeux de cybersécurité de l'Intelligence Artificielle

RÉFÉRENCE 37



DURÉE

**1 jour
Présentiel**

NIVEAU

Initiation

Public

Cette formation s'adresse à un public large, qui souhaiterait avoir un aperçu général des enjeux de cybersécurité autour de l'intelligence artificielle (décideurs, RSSI, managers, professionnels de l'IA,...).

Prérequis

Aucun prérequis

Thématiques

Concepts et définitions de l'IA, Enjeux de cybersécurité de l'IA, Gouvernance et régulation.

Présentation

Cette formation vise à sensibiliser sur les enjeux de cybersécurité dans le domaine de l'intelligence artificielle. Elle aborde en particulier la cybersécurité des systèmes d'IA, en s'appuyant sur des cas pratiques. Les impacts réglementaires (notamment le règlement européen sur l'IA) et le rôle des entités publiques seront également décrits pour avoir une vision complète de la gouvernance à mettre en place lors de l'implémentation d'un système d'IA.

Objectifs

- Comprendre les concepts et définitions autour de l'IA
- Comprendre les principaux enjeux de cybersécurité de l'IA
- Etre en capacité de prendre en considération les risques dans des situations concrètes
- Connaître les obligations légales et les bonnes pratiques recommandées par l'ANSSI

Nouveau

Sensibilisation aux enjeux de cybersécurité de l'Intelligence Artificielle

RÉFÉRENCE 37

Programme

Module 1 : Concepts et définitions

- Origine de l'IA
- Présentation des concepts autour de l'IA
- Définitions d'un système d'IA
- Cas spécifique des LLMs

Module 2 : Gouvernance, régulation et mise en oeuvre

- L'approche par les risques : le cas du règlement européen IA et normes associées
- Rôle des entités étatiques et articulation des réglementations cyber
- Fondamentaux à retenir

Module 3 : Enjeux de cybersécurité liés à l'IA

- Cybersécurité de, par et face à l'IA
- Focus sur les vulnérabilités spécifiques à l'IA
- Cas spécifique des LLMs
- Mesure de sécurité

Module 4 : Cas pratique et recommandations

- Focus sur un SIA parmi plusieurs cas d'usages (assistant bureautique LLM, vidéoprotection, développement logiciel, etc.)





Accès

Transport le plus proche



Esplanade de la Défense



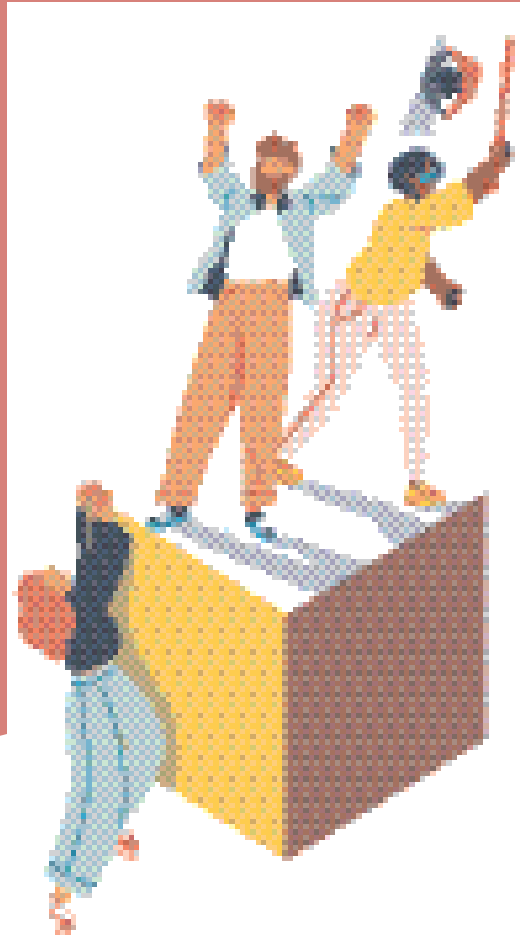
La Défense (Grande Arche)

Accessibilité routière



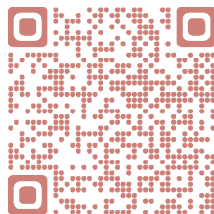
Quai de Dion Bouton
à 200 mètres

Boulevard circulaire au pied
de l'immeuble



Pour plus d'informations :

www.cyber.gouv.fr/administration/formations/



ANSSI

51, boulevard de la Tour Maubourg
75700 PARIS 07 SP

www.cyber.gouv.fr - communication@ssi.gouv.fr



Version 1.0 – Juin 2023