Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Agence nationale de la sécurité des systèmes d'information

Fiches de stage

2015/2016

Le descriptif détaillé de chaque offre est disponible sur le site de l'ANSSI :

www.ssi.gouv.fr

CANDIDATER

Si vous êtes en dernière année de formation et que vous souhaitez candidater sur un des stages proposés, veuillez adresser un courriel ayant pour objet :

- **[STAGE] Candidature de {Nom} {Prénom} {référence du stage}**

A l'adresse suivante :

- recrutement [at] ssi.gouv.fr

Il doit être accompagné de :

- votre CV ;
- une lettre de motivation ;
- une liste maximum de 4 sujets de stage avec les codes correspondants

Si votre candidature retient notre attention, une date d'entretien vous sera proposée par courriel.
A défaut de réponse dans un délai d'un mois, considérez que votre candidature n'a pas été retenue.

Ces stages peuvent nécessiter d'accéder à des informations relevant du secret de la défense nationale, les candidats retenus feront l'objet d'une procédure d'habilitation, au niveau Confidentiel Défense, conformément aux dispositions des articles R.2311-1 et suivant du Code de la défense et de l'IGI n°1300 SGDN/PSE/PSD du 23 juillet 2010.

Pour en savoir plus, et notamment avoir accès à la notice individuelle de sécurité 94A, lire http://www.sgdsn.gouv.fr/site rubrique124.html

SOMMAIRE

FICHES DE STAGE

Mise en place du SSO pour application Android

Supervision applicative

Extraction de données

Ergonomie et portabilité Redmine (stage court)

Agrégateur d'informations - Tableau de bord

Réalisation d'applications pour téléphones Android

Outil de management de projet

Application Mobile - Portail

Etude d'outils d'indexation de code source (Stage court)

Outil de monitoring de versions des applicatifs

Développement d'un webmail avec authentification forte et chiffrement

Moteur d'uniformisation de configuration (stage court)

Ingénierie de trafic et qualité de service pour applications temps réel sur réseaux MPLS

Compression de trafic sur lien satélitaire et 4G (stage court)

Mise en oeuvre d’une architecture de ToIP sécurisée basée sur des briques opensource

Développement d'outils de configuration assistée d'équipements réseau (stage court)

Etat de l’art des pare-feu du marché (stage court)

Solution distribuée de gestion de firewall en environnement hétérogène

Outil de déploiement et de gestion de configurations applicatives sous Linux

Gestion de flotte de terminaux Android sécurisés

Banc de test virtualisé à la demande (IaaS/PaaS)

Migration Windows 7 vers Windows 10

Automatisation de la mise en place d'une chaîne de démarrage sécurisée pour serveur

Emulation et tests automatisés sur Android

Centre Opérationnel en Sécurité des Systèmes d’Information (COSSI)

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Fax 01.71.75.84.00

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2000

Détection de comportements malveillants dans des journaux d'évènements Active Directory

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes, dont des infrastructures s'appuyant sur des outils d'entreprise Microsoft.

Parmi les techniques de détection possibles, l'analyse a posteriori de journaux d'évènements issus de serveurs Active Directory peut permettre de détecter des compromissions d'un système d'information s'appuyant sur ce type d'infrastructure.

La démarche générale consiste à :
• collecter des évènements issus d'un serveur Active Directory sur un serveur central d'analyse ;
• détecter, sur la base de ces évènements, des comportements légitimes, suspects ou malveillants (scénarios prédéfinis, analyse statistique, analyse par la visualisation, etc.).
L'objectif du stage est de :
• étudier le fonctionnement d'Active Directory et le panel d'évènements qu'il est possible de générer pour en tracer l'activité ;
• réaliser un état de l'art des techniques et méthodologies d'analyse existantes ;
• déterminer les types d'évènements pertinents à considérer pour l'analyse ;
• définir et implémenter des stratégies de détection de comportements suspects ou malveillants à partir des évènements collectés.
A l'issue du stage, il est demandé :
• une documentation précisant les types d'évènements collectés, la (les) méthode(s) utilisée(s) pour leur collecte, et les stratégies de détection implémentées ;
• une plateforme documentée validant l'approche.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissances sur le fonctionnement des environnements Microsoft
• Connaissances de base des environnements Linux
• Connaissances de base en Python

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour le fonctionnement des environnements Windows
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2001

Classification de profils d'activité sur des traces système Windows

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes, dont des systèmes Windows.

Parmi les techniques de détection possibles, l'analyse de traces système Windows (lancements de processus, opérations sur les fichiers, opérations réseau, etc.) peut permettre de qualifier des profils d'activité, dans l'optique de déterminer un éventuel caractère suspect ou malveillant.

La démarche générale consiste à :
• collecter des traces système issues du fonctionnement de postes ou serveurs Windows ;
• classer ces traces, en s'appuyant sur des techniques de clustering ;
• identifier les clusters présentant des caractéristiques suspectes ou malveillantes.
L'objectif du stage est de :
• comprendre le contenu d'une trace système Windows ;
• proposer et tester des techniques de classification des traces ;
• analyser les résultats et valider les choix effectués à partir de données fournies.
A l'issue du stage, il est demandé :
• une documentation précisant les techniques de classification étudiées et les tests effectués ;
• une plateforme documentée validant l'approche.

Localisation :
31 quai de Grenelle - 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Connaissances sur le fonctionnement des environnements Windows
• Connaissances en méthodes de classification
• Connaissances en langage C ou Python
• Connaissances de base en réseau (TCP/IP)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour le fonctionnement des environnements Windows
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2002

Détection de comportements système malveillants sous OS mobile

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes. Parmi ceux-ci, les OS mobiles (Android, iOS, etc.) prennent une part de plus en plus importante.

Plusieurs techniques peuvent être mises en oeuvre pour détecter des attaques ou manifestations de compromissions sur des OS mobiles, parmi lesquelles l'analyse statique de formats de fichiers ou de protocoles réseau spécifiques à ces environnements, ou encore l'analyse automatisée en environnement supervisé.

L'objectif du stage est de :
• réaliser un état de l'art des techniques et outils d'attaque d'OS mobiles ;
• réaliser un état de l'art des techniques et outils existants de détection d'attaques et de compromission sur des OS mobiles ;
• proposer une approche de détection innovante et la qualifier dans le temps imparti ;
• développer une preuve de concept de l'approche proposée.
A l'issue du stage, il est demandé :
• une documentation des techniques et outils d'attaque et de détection, de l'approche proposée et des fonctions implémentées ;
• une plateforme documentée répondant aux objectifs du stage.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissances de base en OS mobiles (Android, iOS)
• Connaissances en C et/ou Python, ainsi que les langages de référence des OS mobiles (JAVA, C++, Objective C)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour le fonctionnement des OS mobiles
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2003

Détection de traces d'exploitation de vulnérabilités dans une image mémoire Windows

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes, dont des environnements Windows.

Plusieurs techniques peuvent être mises en oeuvre pour détecter des attaques dans ce cadre, dont l'analyse automatisée d'images mémoire en cas de crash d'applications.

La démarche générale consiste à :
• décoder le format des images générées par le système lors d'un crash applicatif ;
• extraire les informations utiles à l'analyse ;
• qualifier ces informations pour déduire la cause du crash ;
• déterminer les conséquences du crash, en mettant en évidence le cas échéant une tentative d'attaque.
L'objectif du stage est de :
• réaliser un état de l'art des techniques et outils de décodage d'images mémoire Windows issues de crashes applicatifs ;
• proposer des techniques d'analyse des informations contenues dans les images ;
• développer une preuve de concept validant les techniques d'analyse proposées.
A l'issue du stage, il est demandé :
• une documentation des techniques et outils de décodage étudiés, ainsi que des techniques d'analyse proposées ;
• une plateforme documentée répondant aux objectifs du stage.

Localisation :
31 quai de Grenelle - 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Connaissances en systèmes Windows (fonctionnement général, représentation mémoire, etc.)
• Connaissances sur les techniques d'attaque en environnements Windows
• Connaissances sur les outils d'inspection mémoire (debuggers)
• Connaissances d'un langage de programmation (C, python)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour le fonctionnement des environnements Windows
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2004

Classification automatisée de familles de fichiers par construction d'un ADN

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes.

Plusieurs techniques peuvent être mises en oeuvre pour détecter des attaques dans ce cadre, dont l'analyse statique de fichiers. Une technique d'analyse statique est l'identification, par format de fichier, de caractéristiques communes (ADN) permettant la constitution de familles. L'appartenance d'un fichier donné à une famille doit permettre de lui attribuer de facto l'ensemble des résultats d'analyse connus pour n'importe quel membre de cette famille.

L'objectif du stage est de :
• étudier et comprendre un (ou plusieurs) format(s) de fichiers donné(s) ;
• identifier des caractéristiques permettant de construire un ADN pour le (ou les) format(s) considéré(s) ;
• proposer et mettre en application des techniques permettant de classifier un jeu de fichiers selon le (ou les) ADN obtenu(s).
A l'issue du stage, il est demandé :
• une documentation des caractéristiques retenues par format de fichier, ainsi que des techniques de classification proposées ;
• une plateforme documentée validant les objectifs du stage.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissances en C et/ou Python
• Connaissance de techniques de classification de données

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour l'étude de formats de fichiers
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2005

Détection de fichiers malveillants par analyse statique

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir et développer des outils d'analyse afin de détecter d'éventuels fichiers malveillants.

Ces outils ont pour objectif de mettre en évidence :
• des anomalies dans la structure des fichiers par rapport aux spécifications de leur format et par rapport aux usages habituels ;
• des tentatives d'exploitation de vulnérabilités connues.
Pour ce faire, il est nécessaire de spécifier et développer des outils d'analyse (parseurs) pour chaque format considéré.

L'objectif du stage est de développer des outils d'analyse d'un ou de plusieurs formats de fichiers (qui seront précisés au début du stage) et notamment, pour chacun d'eux :
• d'analyser de manière théorique les caractéristiques du format (lecture des spécifications) ;
• d'analyser de manière pratique, à partir d'un ensemble de fichiers de test que le stagiaire se constituera, les usages du format (statistiques sur le respect des caractéristiques théoriques) ;
• de faire un état de l'art des vulnérabilités connues associées au(x) format(s) de fichier ;
• de développer un parseur permettant de chercher dans la structure du fichier toute anomalie, connue ou non.
A l'issue du stage, il est demandé, pour chacun des formats étudiés :
• une documentation précisant les grandes lignes des caractéristiques du format, les particularités d'usages du format par les principaux logiciels générant et/ou lisant ces fichiers, ainsi que leurs différentes vulnérabilités logicielles liées à une mauvaise gestion du format ;
• un parseur du format de fichier permettant d'identifier toute anomalie ou tentative d'exploitation.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissances en C

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Curiosité et envie d'entrer dans les détails des formats de fichiers

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2006

Etude de la robustesse aux évasions d'outils de DPI libres

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir et étudier des outils de détection d'attaques ciblant différents types de systèmes.

Parmi les fonctions offertes par les systèmes de détection d'intrusions réseau, la DPI (Deep Packet Inspection) permet la classification et le décodage de protocoles réseau. Cette fonction, centrale dans les IDS modernes, n'en demeure pas moins sensible aux évasions, permettant à un attaquant d'exploiter les différences qu'il peut exister entre les spécifications des protocoles et leur implémentation dans les fonctions de DPI.

L'objectif du stage est de :
• réaliser un état de l'art des solutions libres de DPI ;
• tester les différentes solutions identifiées et étudier la méthodologie de développement de dissecteurs protocolaires ;
• proposer et mettre en application une ou plusieurs méthodes permettant d'évaluer la robustesse aux évasions des solutions retenues ;
• le cas échéant, proposer des mesures pour pallier ces limitations (détection, correction).
A l'issue du stage, il est demandé :
• une documentation récapitulant l'état de l'art des solutions libres de DPI, les méthodes retenues pour l'évaluation de la robustesse aux évasions, ainsi que les résultats obtenus ;
• une plateforme documentée validant les objectifs du stage.

Localisation :
31 quai de Grenelle - 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Bonnes connaissances en protocoles réseau (TCP/IP et protocoles applicatifs les plus courants)
• Connaissance du fonctionnement général d'un système Linux
• Connaissances en exploitation de vulnérabilités logicielles
• Connaissances en C/C++ (optionnellement Python)
• Connaissance de Scapy (idéalement)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Fort intérêt pour le fonctionnement des protocoles réseaux de l'Internet
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2007

Détection passive de l'évolution de la cartographie d'un réseau

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir et de mettre en oeuvre des outils de détection d'attaques ciblant différents types de systèmes.

Parmi les problématiques relatives à la mise en oeuvre d'outils de détection réseau, la connaissance des évolutions des systèmes d'information supervisés est essentielle, tant pour permettre l'analyse des alertes de sécurité remontées, que pour assurer un paramétrage et une exploitation optimale des solutions. De nombreuses informations de cartographie (topologie, inventaire) peuvent être collectées à partir des flux réseau (IP, OS, services, applicatifs, etc.). Ces informations peuvent permettre d'améliorer la compréhension du système d'information considéré et d'en déduire les évolutions dans le temps.

L'objectif du stage est, à partir d'un ensemble d'informations de cartographie collectées au fil de l'eau (e.g. IP, user-agent, empreintes logicielles, etc.), de :
• définir et valider des profils de référence de l'état du système d'information à un instant initial ;
• proposer et mettre en oeuvre des techniques permettant de mesurer des évolutions des profils de référence dans le temps ;
• qualifier le plus finement possible à l'aide d'inférences ces évolutions (pannes, nouveaux usages, attaques, etc.).
A l'issue du stage, il est demandé :
• une documentation présentant les profils définis et les techniques mises en oeuvre pour mesurer et qualifier les évolutions du système d'information ;
• une plateforme documentée validant les objectifs du stage.

Localisation :
31 quai de Grenelle - 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Connaissances de base en réseau (TCP/IP, protocoles applicatifs de l'Internet, NAT, routage)
• Connaissances en C et/ou Python

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2008

Visualisation et analyse de flux réseau

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Systèmes de détection (BSD) est amené à concevoir des outils de détection d'attaques ciblant différents types de systèmes. Parmi les informations considérées pour qualifier l'activité des systèmes d'information supervisés, les méta-données Netflow offrent une vue macroscopique des communications aux niveaux réseau et transport du modèle OSI.

La démarche générale consiste à :
• collecter des Netflow synthétisant l'activité d'un réseau donné ;
• représenter ces Netflow selon différentes méthodes de visualisation ;
• permettre à un analyste de détecter de manière simple et efficace des comportements suspects et d'investiguer dans les méta-données obtenues.
L'objectif du stage est de :
• comprendre le contenu des méta-données Netflow ;
• établir un état de l'art des outils existants pour visualiser et manipuler des Netflow ;
• proposer des méthodes de visualisation et d'analyse sur la base de Netflow répondant aux besoins d'un analyste ;
• implémenter un outil permettant de valider les propositions.
A l'issue du stage, il est demandé :
• une documentation précisant le cahier des charges retenu, les spécifications techniques, les détails d'implémentation, et le manuel utilisateur ;
• un outil documenté validant l'approche.

Localisation :
31 quai de Grenelle - 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Connaissances de bases en réseau (TCP/IP)
• Langages de programmation Web (PHP, Python, JS, etc.)
• Capacité à comprendre et répondre à un besoin utilisateur
• Bon sens de l'ergonomie d'une IHM

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit, rigueur et autonomie
• Intérêt pour le développement Web et les interfaces homme-machine

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2009

Analyse des traces d'exécution d'outils malveillants sous Windows

Description :
Au sein du Centre Opérationnel SSI, le bureau Réponse aux Incidents est amené à réaliser des analyses de systèmes compromis. Une partie de cette tâche consiste à comprendre le déroulement de l'attaque et à identifier les indices d'exécution d'outils malveillants permettant la prise d'empreinte système, l'exploitation de vulnérabilités ou encore la post-exploitation.
Sous Microsoft Windows, il existe un nombre important d'outils publics de ce type et chacun d'eux laisse des traces différentes suite à leur exécution. Celles-ci, se présentant sous différentes formes (entrées dans les journaux des évènements, MFT, journaux USN, clefs de base de registre, etc.), sont systématiquement analysées et indispensables à la compréhension du scénario d'attaques mené par l'attaquant.

Le stage se déroulera en 3 phases.

• La première phase consistera en un recensement des outils de compromission publics connus ainsi que des commandes système (tels que celles proposées par Powershell) utiles lors d'une intrusion. Cette première démarche pourra être menée avec l'aide du bureau Audit et Inspection du Centre Opérationnel SSI.

• La deuxième phase aura pour objectif d'exécuter sur des plateformes de test les outils et commandes recensés avec les différentes options possibles.

• La dernière phase sera d'identifier et d'analyser les traces d'exécution générées par ces outils et commandes afin d'en extraire des marqueurs système exploitables dans le cadre des nouveaux incidents traités par le bureau Réponse aux Incidents.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• Bonne connaissance de l'environnement technique Windows (ligne de commande, base de registre, MFT, journaux des événements, ...) ;
• Connaissances de quelques techniques/outils de tests d'intrusion sous Windows (pwdump, mimikatz, metasploit, nmap, nirsoft, sysinternals ...) ;
• La maîtrise du PowerShell serait un plus.

Formation :

• Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique
Qualités requises :

• Ouverture d'esprit et rigueur
• Rigoureux(se)
• Autonome et capacité d'investigation
• Savoir construire une démarche structurée

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2010

Analyse forensique d'un système d'information étendu

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Réponse aux incidents (BRI) est régulièrement impliqué dans l'analyse de compromissions impliquant des dizaines de milliers de machines dans des environnements dispersés géographiquement et hétérogènes.

Les technologies habituellement mises en oeuvre (analyse d'images mémoire ou disque) permettent l'analyse très approfondie d'un nombre limité de systèmes. L'objectif de ce stage est de participer au développement de méthodes et d'outils d'analyse complémentaires permettant de passer à l'échelle de plus grands parcs de systèmes compromis.

Le stagiaire devra appréhender les différentes technologies permettant d'extraire les informations d'une machine démarrée et arrêtée impliquant ou non l'installation d'un agent sur les machines, avec leurs avantages et leurs limites.

Le stage se déroulera de la façon suivante :
• réalisation d'un état de l'art des méthodes, techniques et outils existants pour le traitement d'incidents à grande échelle ;
• inventaire des éléments d'information extractibles par la seule utilisation des services réseau offerts par les machines connectées (base de registre à distance, service serveur, WMI, LDAP, etc.) ;
• développement éventuel et tests d'outils spécifiques adaptés à la collecte de ces informations à grande échelle. Pour les informations nécessitant l'exécution d'un agent sur les machines analysées, le stagiaire pourra être amené à participer au développement d'outils adaptés ;
• étude des moyens de collecte et d'analyse permettant d'exploiter les données produites.
A l'issue du stage, il est demandé :
• un état de l'art comparatif des outils, techniques et méthodes disponibles sur le marché dans ce domaine ;
• de proposer ou fournir des outils stables et pertinents de par leurs résultats, en vue de les intégrer aux processus de traitement d'incidents à grande échelle.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance des environnements Windows et Linux
• Connaissance d'un langage de programmation (C, C++, Python, etc.)
• Connaissances dans les domaines de collecte, corrélation et analyse de données

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique.

Qualités requises :

• Curiosité et appétence pour les sujets techniques
• Capacité de rédaction et de synthèse
• Rigueur
• Autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2011

Exploitation des capacités matérielles par les codes malveillants

Description :
Au sein du centre opérationnel de la SSI (COSSI), le bureau Failles et signatures (BFS) est chargé d'assurer une veille sur les codes malveillants. À ce titre, des échantillons de codes sont régulièrement récupérés puis analysés pour :
• déterminer leur comportement et leurs fonctionnalités ;
• proposer des signatures de détection et des mesures de blocage préventif.
Dans ce cadre, le bureau BFS est amené à anticiper les évolutions techniques des codes malveillants et à développer des outils permettant d'assister leurs analyses.

L'objectif de ce stage est de faire l'état des lieux et d'étudier :
• comment les codes malveillants peuvent mettre à profit les capacités offertes par le matériel (GPU, Intel SGX,...) pour se cacher ou rendre leurs analyses plus difficiles ;
• les possibilités permettant de détecter et d'analyser ces codes.
À l'issue du stage, il est demandé :
• un état de l'art décrivant les capacités matérielles qui peuvent être utilisées par les codes malveillants ;
• une documentation précisant de manière détaillée les techniques et outils étudiés ;
• une proposition d'outil ou de méthode permettant de faciliter l'analyse de ces codes ainsi que la réalisation de preuves de concept concernant les technologies analysées.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Pratique des méthodes d'analyse de programme (rétroconception et déboguage)
• Connaissance d'outil(s) d'analyse de code binaire (IDA Pro, OllyDbg, Metasm, Miasm, etc.)
• Connaissance d'un langage de programmation bas niveau (C, ASM, ...)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Curiosité et appétence pour les sujets techniques
• Capacité de rédaction et de synthèse
• Autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S2012

Plate-forme de qualification des outils Windows

Description :
Dans le cadre de ses missions, le bureau audits et inspections est amené a développer des utilitaires devant être déployés sur des systèmes d'information de grande envergure. Afin de s'assurer de la qualité de ses outils, l'ANSSI souhaite se doter d'une plate-forme de test permettant de garantir la bonne exécution d'un programme sur un ensemble de versions de systèmes d'exploitation et de mesurer l'impact de l'exécution du programme sur les systèmes ciblés. Le système d'exploitation Microsoft Windows étant majoritairement utilisé sur les réseaux de postes bureautiques, la plate-forme devra contrôler, dans un premier temps, un parc de machines témoins représentatif de l'ensemble des versions de Windows depuis les noyaux 5.0. Afin de mesurer l'impact sur les systèmes ciblés, le stagiaire sera amené à établir des points de contrôles techniques permettant de déterminer les modifications (sur les fichiers et les clés de registre notamment) suite à l'exécution du programme. La plate-forme devra être utilisable au travers d'une interface Web, à partir de laquelle il devra être possible de transmettre des programmes à tester, de récupérer les résultats produits et de consulter les indicateurs d'impact.

Les objectifs du stage sont de :
• réaliser un état de l'art sur les solutions existantes répondant au besoin. Le stagiaire pourra s'appuyer sur une de ces infrastructures si celle-ci s'avère en adéquation avec les objectifs du stage;
• mettre en place une plateforme de test dans un environnement virtualisé. La plate-forme devra être accessible via une interface Web permettant :
- le déploiement de multiples machines virtuelles avec des configurations personnalisées,
- le déploiement d'outils développés à l'ANSSI,
- le déploiement d'agents effectuant des tâches spécifiques sur les machines virtuelles (traitement et/ou collecte des résultats des outils, contrôle d'intégrité des composants système, etc.),
- la consultation et l'export des résultats d'exécution,
- la visualisation des impacts de l'exécution du programme sur les systèmes cibles.

Localisation :	**Durée :**
31 quai de Grenelle - 75015 Paris	6 à 9 mois

Compétences requises :

• Maîtrise des langages de programmation C/C++, d'un ou plusieurs langages de script aux choix (python, ruby, powershell, etc.) et d'un langage de programmation orienté Web type PHP;
• Connaissance des environnements Windows (la connaissance d'Active Directory serait un plus);
• La connaissance des environnements de virtualisation serait un plus.

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Esprit d'initiative, autonomie, rigueur et curiosité pour le domaine de la sécurité des systèmes d'information

Relations Extérieures et Coordination (RELEC)

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Fax 01.71.75.84.00

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S4000

Graphiste – maquettiste

Description :
Rattaché(e) au graphiste, le/la stagiaire sera amené(e) à :
• réaliser des supports de communication (plaquettes, brochures, affichages, fiches, etc.) de la mise en page à l'impression, en passant par le suivi des étapes de fabrication avec les prestataires ;
• proposer une veille des pratiques de mise en forme innovantes.

Localisation :
Hôtel national des Invalides, 51 boulevard de La Tour-Maubourg (Paris 7e)

Durée :
4 à 6 mois

Compétences requises :

• Bonne maîtrise de la chaîne graphique et les logiciels de PAO, notamment InDesign, Illustrator et Photoshop.

Formation :

• Niveau Bac +2 / +3 - Ecole de graphisme

Qualités requises :

• Créativité, réactivité, esprit d'initiative
• Capacité d'adaptation
• Capacité à travailler de manière autonome et en équipe

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S4001

Chargé(e) de communication interne

Description :
Rattaché(e) au chargé(e) de communication interne, le/la stragiaire sera amené(e) à :
• prendre part à l'activité éditoriale de la communication interne (newsletter, journal interne) en rédigeant des articles ;
• participer activement à l'organisation des évènements internes (séminaires, journée de cohésion, organisation de rencontres trimestrielles, etc) et à leur déroulement ;
• proposer une synthèse des pratiques de communication interne innovantes.

Localisation :	**Durée :**
Hôtel national des Invalides, 51 boulevard de la Tour-Maubourg (Paris 7e)	6 mois

Compétences requises :

• Connaissances en communication interne
• Compétences rédactionnelles et sens de l'écriture journalistique

Formation :

• Niveau Master 1 ou Master 2 - Ecole de communication

Qualités requises :

• Esprit d'initiative, curiosité, créativité
• Capacité à travailler de manière autonome et en équipe
• Aisance relationnelle, capacité d'adaptation et d'organisation

Sous-Direction Expertise (SDE)

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Fax 01.71.75.84.00

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S3000

Développement d'un algorithme de scoring pour l'estimation du niveau de sécurité d'un produit qualifié

Description :
La qualification d'un produit de sécurité se base sur une évaluation initiale CSPN ou Critères Communs. Le suivi de sécurité de ce produit (impact de nouvelles CVE notamment) est pris en charge par un gestionnaire SSI qui peut ordonner un déclassement du produit dans le catalogue des produits qualifiés ou exiger la réouverture de tâches d'évaluation (surveillance) à l'industriel.

Afin de guider le gestionnaire de risque SSI dans ses choix, une estimation du niveau d'impact des nouvelles vulnérabilités sur les produits est nécessaire. Le stagiaire aura ainsi la charge d'établir un un algorithme de scoring faisant la synthèse de l'impact de multiples sources ouvertes (CVE...) ou fermées (rapport d'évaluation) sur le niveau de sécurité d'un produit, permettant ainsi de connaître en temps réel la criticité d'une correction vis-à-vis des vulnérabilités présentes et non encore traitées par le fabricant dans le cadre d'un processus de veille mis en place par l'Agence.

Le stagiaire aura la charge de définir une maquette sous Access et VBScript implantant cet algorithme via l'import des CVE publics pour une liste de produits donnés, l'évaluation de la criticité de chacun d'entre eux, et la navigation sur une interface ergonomique.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 mois

Compétences requises :

- Connaissance des bases de vulnérabilité courantes (CVSS,...)
- Connaissance des bases de données,
- Connaissance en mathématiques appliquées, statistique et datamining
- Compétences Access + VBScript pour prototyper

Formation :

- Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique

Qualités requises :

- Rigoureux(se)
- Autonome
- Aisance quant à la restitution écrite et orale des travaux

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S3001

Conception d'une trame d'audit développeur pour la qualification élémentaire

Description :
Le processus de qualification élémentaire se base sur le processus d'évaluation CSPN. Ce dernier ne comporte pas de volet audit des développeurs, qui reste nécessaire afin d'établir un certain de niveau de confiance dans le processus de développement du produit et de sa chaine logistique. Le stagiaire aura à établir une trame d'audit s'inscrivant dans le processus de qualification actuel afin de répondre à ce besoin. Le stagiaire tiendra compte dans ses travaux tout autant de l'audit initial, tout comme les audits de suivi de renouvellement. A l'issue du stage, un audit pilote pourra être conduit chez un industriel de confiance.

Localisation :
31, quai de Grenelle – 75015 Paris

Durée :
3 mois

Compétences requises :

- audit organisationnels
- qualité logicielle
- sécurité des développements, chaine logistique

Formation :

- Stage d'école d'ingénieur ou formation universitaire en sécurité informatique (bac +4)

Qualités requises :

- Ouverture d'esprit et rigueur
- Rigoureux(se)
- Autonome
- Aisance quant à la restitution écrite et orale des travaux

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S3002

Caractérisation des conséquences d'une modification du flux de contrôle Java Card

Description :
L'usage des cartes à puce est ancré dans notre vie quotidienne. Nous en utilisons régulièrement pour téléphoner ou payer et elles contiennent des informations sensibles dont non seulement le stockage mais aussi la manipulation des données doit être sécurisée. Ce travail de sécurisation est rendu difficile par la nature des carte à puce qui peuvent être vus comme des petits ordinateurs.

Pour simplifier le processus de développement des applications embarquées, la technologie Java a été portée dans les cartes à puce. A l'instar de Java, les applications Java Card sont indépendantes de l'architecture matérielle et elles sont exécutées dans un bac à sable garantissant un haut niveau de sécurité. Actuellement, cette technologie est utilisée dans la grande majorité des cartes à puce du commerce.

La protection des biens sensibles présents sur la carte (informations bancaires, données de santé, etc.) est donc essentielle, afin d'empêcher un attaquant de cloner une carte ou d'exploiter illégalement les secrets qu'elle renferme. Les fabricants de composants doivent donc évaluer la robustesse de l'implémentation des machines virtuelles JavaCard afin d'identifier des vulnérabilités potentielles avant qu'elles ne soient exploitées par des attaquants.

Le Laboratoire de Sécurité des Composants (LSC) de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) travaille à la validation et à l'amélioration des contre-mesures aux attaques logicielle contre la plateforme Java Card. Dans ce contexte, le LSC propose de caractériser les conséquences d'une modification du flux de contrôle sur le fonctionnement de la machine virtuelle Java Card. Le but est d'évaluer la sécurité d'une implémentation de la plate-forme Java Card vis à vis des attaques par modification de flux d'exécution afin de mettre en place des contre-mesures adéquates. Une modification du flux d'exécution à lieu lorsqu'une portion de code malveillant est exécutée amenant le programme légitime dans un état inattendu. Une contre-mesure efficace doit donc détecter toutes modifications illégitimes.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	5 à 6 mois

Compétences requises :

- Connaissances sur la technologie Java Card
- Connaissances en solveur de contraintes

Formation :

- Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique

Qualités requises :

- Ouverture d'esprit et rigueur
- Autonome
- Aisance quant à la restitution écrite et orale des travaux

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S3003

Analyse de sécurité d'un protocole SCADA

Description :
Au sein de la sous-direction Expertise (SDE), le laboratoire sécurité des réseaux et des protocoles (LRP) a notamment pour mission d'étudier les protocoles industriels afin d'améliorer leur sécurité.

Dans les systèmes industriels, une notion importante est la sûreté de fonctionnement. Elle recouvre différentes propriétés souhaitées comme la fiabilité, la maintenabilité, la disponibilité et la sécurité des biens et des personnes. Cela englobe donc en particulier leur capacité à se prémunir contre des défaillances techniques et, le cas échéant, à garantir le maintien du système dans un état sûr lorsqu'une telle défaillance intervient. Historiquement, les systèmes industriels n'ont pas été conçus pour se défendre contre des actes malveillants et la sûreté de fonctionnement n'inclut pas, à ce jour, la cybersécurité

Par ailleurs, certaines spécificités techniques des systèmes industriels ne permettent pas d'appliquer simplement les bonnes pratiques de sécurité des systèmes d'information. Par exemple, les contraintes fortes en matière de ressources ou de temps de réponse dans certains cas pourraient nécessiter l'usage de cryptographie adaptée.

L'objectif de ce stage est d'étudier un protocole réseau qui apporte des garanties fortes en matière de sûreté de fonctionnement mais n'intègre aucun mécanisme de cybersécurité.

Le stage sera ainsi l'occasion de relever certains défis de conception pour lesquels le stagiaire sera amené à approfondir ses compétences théoriques et pratiques sur des protocoles réseau. Par ailleurs, le stage pourra inclure une part importante de développement, notamment avec Scapy. Enfin, il pourra comporter une partie plus théorique avec la possibilité de concevoir des contre-mesures impliquant notamment de la cryptographie.

Les jalons du stage sont donc :

• l'étude détaillée d'un protocole de sûreté de fonctionnement (PROFIsafe, DeviceNet Safety, etc..) ;

• l'identification des scénarios d'attaque entraînant une mise en défaut des mécanismes de sûreté de fonctionnement ;

• la réalisation une preuve de concept d'un ou de plusieurs de ces scénarios avec Scapy sur une plateforme industrielle de test ;

• la proposition d'évolutions du protocole ou des recommandations de mise en oeuvre.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	5 à 6 mois

Compétences requises :
• Très bonne connaissance du langage Python ;

Formation :

• Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique

Qualités requises :

• Curiosité technique ;

• Capacité d'analyse et esprit critique ;

• Méthodologie et rigueur ;

• Aisance quant à la restitution écrite et orale des travaux (pour des présentations internes et externes).

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S3004

Développement de démonstrations de cybersécurité à destination des enseignants en informatique

Description :
Le projet CyberEdu a pour objectif d'insérer des notions de cybersécurité dans l'ensemble des formations en informatique de France. Pour cela, des guides ainsi que des supports de cours rédigés par des enseignants-chercheurs, de différents niveaux (licence et master), ont été mis à disposition par l'ANSSI. Des stages de sensibilisation à destination des enseignants-chercheurs ont également été mis en place deux fois par an.

Afin d'illustrer les compétences de sécurité que les étudiants doivent acquérir, le stagiaire aura la charge d'identifier et de réaliser des démonstrations sur des vulnérabilités connues qui seront diffusables aux enseignants en informatique. A terme, les démonstrations doivent pouvoir être mises en place facilement dans les établissements d'enseignement supérieur qui le demandent (par exemple, des machines virtuelles mettant en œuvre une attaque de type man-in-the-middle ou des démonstrations mettant en évidence la présence de données en clair dans de nombreux protocoles).

Au cours du stage, le stagiaire devra échanger avec les enseignants pour connaître les besoins et identifier les ressources mobilisables. Il pourra également s'appuyer sur les ressources de l'ANSSI pour monter des démonstrations pilotes.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	4 à 6 mois

Compétences requises :

• Connaissance des bases des vulnérabilités courantes
• Appétence pour la pédagogie

Formation :

• Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique

Qualités requises :

• Rigueur
• Autonome
• Aisance quant à la restitution écrite et orale des travaux

Sous-Direction Systèmes d’Information Sécurisés (SIS)

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Fax 01.71.75.84.00

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1000

Mise en place du SSO pour application Android

Description :
Le système d'exploitation Android, de par son usage principal, n'a pas été prévu pour permettre des mécanismes d'authentification classiquement présents dans les entreprises. De plus, la multitude d'applications qui deviennent accessibles depuis un smartphone nécessite des solutions de SSO (Single Sign On), à la fois pour des raisons d'ergonomie d'usage et pour une plus grande facilité d'administration des applications.

Par exemple, le protocole Kerberos qui répond à cette problématique est massivement utilisé sur les parcs d'ordinateurs. Le but du stage est, à partir des mécanismes et logiciels conçus pour les ordinateurs, de concevoir une solution permettant un accès authentifié transparent aux applications depuis un terminal Android.

De manière plus détaillée, le stage consistera à modifier le framework et certaines applications (Contacts, E-mail…) pour qu'ils supportent le SSO.

Les modifications du framework et des applications seront faites de façon à faciliter la maintenance lors des futures mises à jour d'Android.

Les livrables attendus consistent en
• une documentation descriptive du fonctionnement de la solution
• un prototype fonctionnel
• la documentation de la manière dont ont été prises en compte les problématiques de maintenance de la solution, notamment lors du changement de version d'Android.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• JAVA, C
• Connaissance de base d'Android
• Connaissance de base de Kerberos

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1001

Supervision applicative

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est chargé de la conception, de la réalisation et des évolutions de solutions applicatives sécurisées.

Le stage porte sur la conception d'une solution de supervision applicative.

L'outil de supervision doit :
• s'insérer dans un écosystème applicatif hétérogène
• s'intégrer dans la plate-forme de supervision de l'ANSSI
• vérifier que le service est rendu pour les utilisateurs, par exemple
  - les contenus dynamiques se mettent bien à jour
  - les requêtes retournent des résultats cohérents
  - l'ajout d'information est bien effectif
• être le moins intrusif possible.
• pouvoir accéder à des services nécessitant une authentification forte
• fournir une visibilité globale et contextuelle quand à la qualité de service
Les livrables attendus sont :
• Un état de l'art des solutions existantes
• les documents d'architecture et de conception du système
• une maquette fonctionnelle et le packaging correspondant facilitant son installation
• la documentation technique et fonctionnelle

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Connaissance des langages WEB (HTML, JavaScript, AJAX, CSS)
• Connaissance des différents mécanismes d'authentification (Certificat, Kerberos, ...)
• Connaissance des bases de données (SQL)
• Notions en administration système Linux (fonctionnement d'un daemon, ...)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
Qualités requises :

• Curiosité et autonomie
• Ouverture d'esprit et rigueur

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1002

Extraction de données

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est chargé de la conception, de la réalisation et des évolutions de solutions applicatives sécurisées. L'ANSSI opère différents SI sur lesquels s'exécute un grand nombre de services hétérogènes. Afin d'établir des métriques sur l'utilisation et la santé de ces SI, il est nécessaire d'extraire les informations produites par ou pour les différents services pour les fournir à un système décisionnel. L'objectif du stage est de proposer un système modulaire, extensible et autonome permettant l'extraction et la recherche de données. À l'issue des traitements par le système, les données pourront être fournies en substrat à un ETL. La solution proposée devra être modulaire et extensible (par exemple basé sur un système multi-agent, des plugins...).

Les livrables attendus sont :
• les documents d'architectures et de conception du système
• une maquette fonctionnelle et son packaging simplifiant son installation
• la documentation technique et fonctionnelle

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, Python, ...)
• Connaissance de plusieurs formats de données structurés et non structurés (XML, JSON, CSV, ...)
• Connaissance en modélisation (UML, ...)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Curiosité et autonomie
• Ouverture d'esprit et rigueur

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1003

Ergonomie et portabilité Redmine (stage court)

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est en charge de la conception, de la réalisation et des évolutions de solutions sécurisées proposées aux différents services de l'État.

Les applicatifs déployés sur ses systèmes peuvent être utilisés sur un large panel de terminaux (ordinateur, tablette, smartphone). Le but du stage est de proposer un thème ergonomique pour l'outil Redmine.

Le thème proposé devra :
• utiliser les principes du responsive design ;
• être compatible avec les différents navigateurs (bureautique et mobile) ;
• être ergonomique et agréable.
Les livrables attendus sont :
• les documents de conception
• le thème
• la documentation fonctionnelle et technique

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 5 mois

Compétences requises :

• Bonne connaissance des langages WEB (HTML, JavaScript, CSS)
• Connaissance du langage de programmation Ruby
• Notions d'ergonomie

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
• Niveau Bac +2 / +3 - Ecole de graphisme

Qualités requises :

• Créativité
• Ouverture d'esprit et rigueur

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1004

Agrégateur d'informations - Tableau de bord

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est chargé de la conception, de la réalisation et des évolutions de solutions applicatives sécurisées.

Le bureau Applicatif souhaite intégrer dans plusieurs de ses outils des tableaux de bord. Le stage consiste à proposer une solution de restitution graphique intégrable aux applicatifs existants et futurs.

Cette bibliothèque devra :
• supporter plusieurs formats de données en entrée (XML, XLS, CSV, JSON, ...)
• être capable de générer des substrats de l'information prise en entrée
• proposer plusieurs indicateurs possibles à partir d'une même source de données (camembert, histogramme)
• fournir différents rapports sur un ou plusieurs tableaux de bord
• être ergonomique et agréable
Les livrables attendus sont :
• état de l'art
• conception d'une solution
• réalisation d'un prototype fonctionnel
• la documentation utilisateur et développeur

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Connaissance des langages WEB (HTML, JavaScript, CSS)
• Connaissance de plusieurs format de données structuré et non structuré (XML, JSON, CSV, ...)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Un goût pour l'ergonomie
• Ouverture d'esprit et rigueur

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1005

Réalisation d'applications pour téléphones Android

Description :
Le principal attrait des smartphones actuellement est l'existence d'une multitude d'applications permettant un usage très large de l'appareil. Cependant, une part non négligeable des applications présentes sur les "markets" sont dangereuses pour l'équipement ou les données qu'il contient, quelle que soit l'origine des vulnérabilités (malveillantes ou pas).

Certaines applications sensibles nécessitent donc une maîtrise forte, et pour cela la disponibilité du code source pour qu'il puisse être audité.

Le stage consiste à développer une ou plusieurs applications en fonction des connaissances et des compétences du stagiaire. Ce dernier veillera à respecter les recommandations de Google pour le design d'applications (fluidité, ergonomie, qualité visuelle de l'application...).

Quelques exemples d'applications qui pourront être développées:
• application de prise de notes ;
• lecteur de code barre 1D/2D (Code QR, Datamatrix...). Générateur de la vcard personnelle en code barre 2D ;
• Reconnaissance (via une librairie OCR) des champs d'une carte de visite papier pour ajouter les données à l'application Contacts ;
• Scanner des documents à partir de l'appareil photo;
• Outils réseaux (couverture Wi-Fi, qualité de la connexion...)...
Cette liste n'est pas exhaustive : le candidat pourra proposer des idées d'application lors de l'entretien.

Pour chaque application, le livrable est constitué de:
• le code source de l'application et des éléments (Graddle, Ant...) permettant sa compilation;
• la documentation de conception de l'application;
• la documentation utilisateur et administrateur le cas échéant.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• JAVA
• Connaissances de base d'Android

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Un intérêt pour l'ergonomie sera apprécié

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1006

Outil de management de projet

Description :
Dans le cadre de ses activités, l'ANSSI cherche à optimiser son processus de gestion de projet. Ce stage a pour but de développer un outil de pilotage de projets en prenant en compte la reprise de l'existant et des solutions actuellement déployées.

L'outil devra permettre :
• la restitution des informations sous forme de tableau et de graphiques (Diagramme GANT, Planning ...)
• gérer un portefeuille projets
• gérer un projet
• gérer les priorités et prérequis des tâches dans le temps ()
• permettre une communication efficace entre les intervenants des projets
• proposer une granularité adéquate et contextuelle pour chaque projet
• être ergonomique
• disposer d'une approche responsive design
Les livrables attendus sont :
• les documents d'architecture et de conception
• une maquette fonctionnelle
• la documentation utilisateur et administrateur

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Connaissance des processus de gestion de projet

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Organisation
• Notion d'ergonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1007

Application Mobile - Portail

Description :
Dans le cadre du développement de la mobilité sur les SI, l'ANSSI souhaite mettre en place un portail applicatif mobile permettant de mettre facilement à disposition l'ensemble des services présents sur le système et accessibles par l'utilisateur.

Les plates-formes suivantes doivent être supportées :
• Android : Smartphone, Tablette ;
• Windows ;
• Linux.
Afin de faciliter les développements, les frameworks du type Appcelerator, Titanium, Cordova ou Haxe pourront être utilisés. La solution devra permettre facilement l'ajout d'un nouveau service.

Les livrables attendus sont :
• les documents d'architectures et de conception du système
• le code source de l'application
• la documentation utilisateur et administrateur

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• JAVA
• Connaissance des langages WEB (HTML, JavaScript, CSS)
• Connaissances de base d'Android

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Notion d'ergonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1008

Etude d'outils d'indexation de code source (Stage court)

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est chargé de la conception, de la réalisation et des évolutions de solutions applicatives sécurisées.

Afin de faciliter le travail de ses développeurs, l'ANSSI recherche un stagiaire souhaitant travailler sur le sujet des solutions d'indexation de code.

L'objectif de ce stage consiste à faire un état des lieux des différentes solutions permettant d'indexer et de parcourir efficacement des codes sources de taille importante. Le stagiaire documentera les avantages et inconvénients des différentes solutions existantes proposera celle la plus à même de remplir les besoins des développeurs de l'ANSSI.

Le code source d'Android sera pris comme exemple pour implémenter un démonstrateur de la solution privilégiée lors de l'état de l'art.

Les livrables attendus sont :
• les documents d'architectures et de conception du système;
• une maquette fonctionnelle et son packaging simplifiant son installation;
• la documentation utilisateur et administrateur.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	2 à 3 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Connaissance de base de l'environnement GNU/Linux
• Connaissance de base d'Android préférable

Formation :

• Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Curiosité technique

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1009

Outil de monitoring de versions des applicatifs

Description :
Dans la mise en oeuvre d'un système d'information, connaître les équipements impactés par une mise à jour de sécurité est un élément primordial.

Le stage porte sur la réalisation ou l'intégration d'une application effectuant le monitoring des versions des différents applicatifs (ex: apache, tomcat, php, java, wiki, wordpress ...) installés sur le système d'information. L'outil doit permettre de comparer les versions du parc avec les différentes sources de référence (dépôts des distributions, sites officiels ...).

Le livrable attendu est constitué de:
• la réalisation d'un état de l'art comparatif des solutions existantes;
• la conception et développement d'un prototype fonctionnel;
• le packaging correspondant afin de faciliter les déploiements;
• la rédaction d'une documentation technique de la solution proposée;
• la rédaction d'une documentation utilisateur.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Bonne connaissance des technologies Web (Javascript, HTML5....)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1010

Développement d'un webmail avec authentification forte et chiffrement

Description :
Au sein de la sous-direction Systèmes d'information sécurisés (SIS), le bureau Applicatif est en charge de la conception, de la réalisation et des évolutions de solutions sécurisées proposées aux différents services de l'Etat.

Le stage porte sur le développement d'un webmail sécurisé accédant à un service de messagerie électronique.

Les travaux devront intégrer les besoins suivants:
• Authentification forte de l'utilisateur (carte à puce);
• Chiffrement et déchiffrement des messages sur le poste client;
• Accès sécurisé au serveur de messagerie.
Le stage se déroulera de la façon suivante:
• Réalisation d'un état de l'art comparatif des solutions existantes;
• Conception et développement d'un prototype fonctionnel et son packaging simplifiant son installation;
• Rédaction des documentations technique et fonctionnelle de la solution proposée.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Maitrise d'un langage de programmation (PHP, Java…)
• Développement d'applets Java
• Bonne connaissance des technologies Web (Javascript, HTML5….)
• Bonnes notions de cryptographie (IGC, carte à puce, S/MIME…)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
Qualités requises :

• Ouverture d'esprit et rigueur
• Autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1011

Moteur d'uniformisation de configuration (stage court)

Description :
Au sein d'une même desserte, les configurations des équipements réseaux sont censées être similaires voire dérivées d'un modèle de configuration. Toutefois, la vie du système d'information peut conduire à des divergences qui n'auraient pas été reportées. Un moteur d'uniformation permettrait, à partir d'une configuration modèle, d'extraire les différences entre les configurations analysées et proposer des modifications à apporter.

Dans le cas où un outil réalisant en partie de ces fonctionnalités est identifié durant l'état de l'art, le stage se focalisera sur l'ajout des fonctionnalités manquantes. Le livrable attendu à la fin du stage est la sélection, l'adaptation ou le développement d'un tel programme ainsi que son packaging simplifiant son installation. La documentation correspondante, utilisateur comme développeur est également attendue.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 4 mois

Compétences requises :

- Connaissance d'un langage de programmation ou de scripting (python, C...) ;
- Connaissance de l'environnement GNU/Linux ;
- Bases en administration réseau ;
- Un bagage réseau serait un plus.

Formation :

- Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique.

Qualités requises :

- Ouverture d'esprit et rigueur ;
- Capacité à retranscrire un besoin métier ;
- Automonie.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1012

Ingénierie de trafic et qualité de service pour applications temps réel sur réseaux MPLS

Description :
Afin de fournir un maximum de services via un même réseau, plusieurs applications peuvent utiliser un même lien télécom. L'utilisation concurrente de ces applications peut poser un problème de qualité de service, notamment en présence d'applications temps réel (téléphonie, visioconférence…).

L'objectif de ce stage est de réaliser un état de l'art et d'étudier les technologies d'ingénierie de trafic (*traffic engineering*), de qualité de service et de réservation de ressources afin de s'assurer que l'application bénéficiera du minimum de ressources nécessaires. Le stagiaire pourra également s'orienter sur des solutions de routage réalisé par la QoS. Cette étude sera argumentée par la réalisation d'une preuve de concept qui implémentera la solution proposée.

Le livrable attendu est :
• une documentation de l'étude ;
• un modèle de configuration à appliquer sur les équipements réseaux pour implémenter les fonctions de la solution ;
• une documentation administrateur.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 mois

Compétences requises :

• Bonnes connaissances des protocoles WAN (p.ex. MPLS) ;
• Connaissances des protocoles réseaux de qualité de service ;
• Connaissances en visioconférence ou téléphonie ou autre application en temps réel ;
• Compétences réseaux.

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur ;
• Autonomie ;
• Esprit de synthèse ;
• Écoute.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1013

Compression de trafic sur lien satélitaire et 4G (stage court)

Description :
Dans le cadre de ses missions l'ANSSI offre des solutions de communication sur tout type de réseaux. Cependant certains réseaux très spécifiques utilisés en mobilité imposent d'étudier des techniques d'optimisation de la bande passante tout en prenant en compte les contraintes de ces réseaux, notamment en termes de pertes de paquets et de latence. Un des moyens d'optimiser ces trafics est de compresser les données directement sur les équipements de routage. Il sera demandé de réaliser un état de l'art des technologies adaptées, et de présenter une solution sous forme de rapport, et de preuve de concept.

Localisation :
31, quai de Grenelle – 75015 Paris

Durée :
3 à 4 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, Python, ...)
• Très bonnes connaissances en réseau :
  - protocoles de routage dynamique (OSPF, RIP, BGP, ...) ;
  - IPv4/IPv6 (en détail) ;
  - GRE, UDP, TCP ;
  - problématiques WAN.

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur ;
• Autonomie ;
• Anglais technique ;
• Bonnes qualités rédactionnelles.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1014

Mise en oeuvre d'une architecture de ToIP sécurisée basée sur des briques opensource

Description :
Depuis quelques années, la téléphonie fixe d'entreprise, anciennement numérique voire analogique, évolue naturellement vers le tout IP : on parle alors de téléphonie sur IP ou de ToIP. Un certain nombre de protocoles ont émergé des constructeurs ou des instances de normalisation, tel que le couple SIP/RTP ou leurs composantes sécurisées qui tend fortement à s'imposer dans le domaine de la ToIP.

L'objectif de ce stage est de définir et mettre en oeuvre une architecture ToIP sécurisée basée sur ces protocoles en utilisant des briques opensource et les équipements réseaux fournis (routeurs / pare-feu).

Le déroulement attendu du stage est le suivant :
• Faire un état de l'art des briques opensource permettant de réaliser un système ToIP fonctionnel, en s'appuyant notamment sur des études existantes :
  - identification des différentes composantes d'une infrastructure ToIP ;
  - comparaison des briques opensource entre elles aussi bien au niveau fonctionnel que sécurité.
• Proposer une architecture de ToIP sécurisée :
  - identification et catégorisation des menaces qui peuvent impacter une telle architecture.
• Mettre en oeuvre cette architecture :
  - installation / configuration ;
  - tests de performance ;
  - vérification des mesures de sécurité déployées.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 mois

Compétences requises :

• Bonne connaissance des protocoles SIP/RTP ou intérêt fort pour comprendre ces protocoles ;
• Notions de sécurité informatique (chiffrement TLS, menaces de type DoS, etc.) ;
• Connaissance de langages de script (shell, Python, ...) ;
• Aisance en environnement Linux (compilation, administration courante, ...) ;
• Bon anglais technique.

Formation :

• Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique

Qualités requises :

• Ouverture d'esprit et rigueur ;
• Rigoureux(se) ;
• Autonome ;
• Aisance quant à la restitution écrite et orale des travaux.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1015

Développement d'outils de configuration assistée d'équipements réseau (stage court)

Description :
Dans le cadre de ses missions, l'ANSSI est amenée à fournir des modèles de configurations à des entités chargées de configurer un grand nombre d'équipements hétérogènes. Afin de configurer ces équipements le plus facilement possible et en minimisant les erreurs utilisateur, un outil d'assistance est nécessaire. L'objectif de ce stage est de développer ou de modifier un tel outil qui permettra, à partir d'une configuration modèle, de configurer l'équipement réseau. Parmi les fonctionnalités souhaitées :
• vérification de version avant configuration ;
• configurations à conditions ;
• retour d'erreur.
Le livrable attendu est le développement des fonctionnalités et son packaging simplifiant son installation. Il sera dûment documenté tant du point de vue utilisateur que développeur.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 mois

Compétences requises :

• Connaissance d'un langage de programmation ou de scripting (python, C...) ;
• Connaissance de l'environnement GNU/Linux ;
• Bases en administration réseau ;
• Un bagage réseau serait un plus.

Formation :

• Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur ;
• Capacité à retranscrire un besoin métier ;
• Automonie.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1016

Etat de l'art des pare-feu du marché (stage court)

Description :
Il existe actuellement de nombreuses technologies de filtrage allant des plus rudimentaires aux plus complexes. Dans le cadre de ses missions l'ANSSI a besoin de protéger ses moyens télécom notamment avec des pare-feu qualifiés. Aussi, réaliser un état de l'art de toutes les fonctionnalités de sécurités présentes sur le marché des pare-feu permettra à l'ANSSI de maintenir à jour ses architectures télécom et d'anticiper les prochaines évolutions nécessaires. L'objectif du stage est donc d'étudier et comparer un ensemble de moyens de filtrage (opensource ou privés) puis de tester leur intégration dans une architecture préexistante.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 mois

Compétences requises :

- Bonnes connaissances réseaux dont protocoles IPv4/IPv6, TCP/UDP ;
- Bonnes connaissances en sécurité ;
- Connaissances Linux et iptables.

Formation :

- Bac +5 - Ecole d'ingénieur ou formation universitaire en sécurité informatique.

Qualités requises :

- Ouverture d'esprit et rigueur ;
- Rigoureux(se) ;
- Autonome ;
- Aisance quant à la restitution écrite et orale des travaux.

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1017

Solution distribuée de gestion de firewall en environnement hétérogène

Description :
Dans le cadre de ses activités, l'ANSSI est amenée à administrer un parc hétérogène de serveurs (Linux, BSD, Windows, etc.). Ce stage a pour but de concevoir ou d'identifier un outil existant offrant les fonctionnalités suivantes:
• distribution sécurisée de configurations de parefeux sur des systèmes hétérogènes (à minima Linux et BSD) avec support du retour d'une configuration dans un état précédent (rollback) ;
• récupération de la configuration du parefeu des systèmes en production ;
• validation de la configuration d'un parefeu pour vérifier le bon respect des règles d'une politique de sécurité ;
• interface d'administration Web moderne ;
• support de plusieurs rôles et groupes gérés centralement afin de séparer les privilèges ;
• intégration avec les méthodes de virtualisation légère (par ex. LXC) : le parefeu peut être configuré sur le système hôte et invisible au système invité.
Dans le cas où un outil réalisant en partie de ces fonctionnalités est identifié durant l'état de l'art, le stage se focalisera sur l'ajout des fonctionnalités manquantes et l'intégration de l'outil dans le SI de l'agence.

Le livrable attendu à la fin du stage est la sélection, l'adaptation ou le développement d'un agent (partie logicielle présente sur les serveurs permettant la configuration du parefeu), du serveur et de la documentation correspondante.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un ou plusieurs langages de programmation (C, Python, Java, ...)
• Bonnes notions en administration système Linux et BSD.
• Bonne connaissance des parefeux applicatifs (netfilter, packet filter, ...)

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit
• Rigueur
• Capacité à travailler en équipe
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1018

Outil de déploiement et de gestion de configurations applicatives sous Linux

Description :
La gestion d'un parc de taille importante de machines nécessite d'avoir des outils adaptés afin de garder une base de configuration homogène pour l'ensemble des applications métiers des utilisateurs. Dans un environnement Linux, les éléments de configuration sont principalement paramétrés selon deux modes: de manière globale pour tout un système, ou délégués à chaque utilisateur. Dans certain cas, une combinaison de ces deux modes est utilisée. Il s'agit ici de créer un nouveau niveau de configuration intermédiaire permettant à un administrateur d'appliquer un ensemble de paramètres maîtrisés à un utilisateur ou à un groupe d'utilisateur. Cette nouvelle flexibilité pour l'administrateur permet de rajouter de nouveaux éléments de configuration à une application sans pour autant annuler toutes les modifications qu'auraient pu apporter les utilisateurs à celle-ci. Par exemple, il serait possible d'ajouter de manière transparente une nouvelle boite email à un utilisateur, restreindre des éléments de sa configuration (par ex. limiter les méthodes d'authentification), ou de configurer des services spécifiques uniquement pour un sous-ensemble des utilisateurs.

Ce stage porte sur le développement de l'ensemble des éléments permettant de réaliser ce module de configuration:
• développement d'un couple agent et serveur de configuration permettant de tirer parti de cette nouvelle source de configuration et de distribuer les configurations par le réseau, ceux-ci devront s'intégrer avec les outils existants à l'agence ;
• peuplement de la configuration initiale par défaut pour les applications métiers ;
• support de l'évolution incrémentale des configurations ;
• modification des applications métiers existantes pour ajouter le support du nouveau système de configuration ;
• l'ensemble de l'architecture devra être porté sur le système d'exploitation développé par l'agence (CLIP).
La partie sécurité de la solution est très importante et revêtira plusieurs aspects:
• durcicement logiciel des agents et des serveurs de configuration ;
• garantie de l'authenticité et de l'intégrité de l'ensemble des configurations ;
• protection de la communication entre les différents éléments.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, Python, PHP, Java, ...)
• Bonnes connaissances systèmes et d'architecture

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
• Stage de fin d'études

Qualités requises :

• Ouverture d'esprit et rigueur
• Curiosité et autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1019

Gestion de flotte de terminaux Android sécurisés

Description :
L'ANSSI développe et déploie des terminaux mobiles sécurisés sous le système d'exploitation Android. Le but du stage est d'améliorer le système de gestion de flotte pour ces terminaux. La solution doit notamment permettre la centralisation sur un serveur des caractéristiques de chacun des terminaux (utilisateur, identifiant, version logicielle, etc.) et la passation de commandes vers le terminal (modification de la configuration réseau...). Le développement se concentrera sur la partie client Android qui communiquera avec un serveur de gestion existant.

Le stage comportera une partie d'étude sur l'état de l'art des solutions existantes, tout en évaluant l'impact sur la sécurité des terminaux. La seconde partie sera la réalisation de la solution retenue.

Le livrable attendu à la fin du stage est
• le développement d'un client ou l'adaptation d'un client déjà existant repondant aux contraintes de sécurité de l'ANSSI;
• l'adaptation de la partie serveur de l'interface de gestion de flotte déjà existante;
• le packaging correspondant afin de simplifier le déploiement;
• les documentations de conception, utilisateur et administrateur de la solution.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	6 à 9 mois

Compétences requises :

• Connaissance d'un ou plusieurs langages de programmation (C, JAVA, ...)
• Notions en sécurité informatique
• Connaissance du système d'exploitation Android

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
• Stage de fin d'études

Qualités requises :

• Ouverture d'esprit et rigueur
• Curiosité et autonomie

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1020

Banc de test virtualisé à la demande (IaaS/PaaS)

Description :
Dans le cadre de ses activités, l'ANSSI développe des chaines d'accès sécurisé permettant à ses terminaux mobiles de se raccorder à certains SI. Ces plateformes comportent plusieurs machines sous différents systèmes d'exploitation. Afin d'accélérer la mise au point de nouvelles versions, les tests s'effectuent sur des machines virtuelles. Le but du stage est de concevoir un banc de test permettant de gérer efficacement ces ensembles de machines virtuelles. La réalisation attendue est un système qui permettra d'instancier et de mettre en réseau des ensembles de machines virtuelles. Intégré au SI, afin de permettre la collaboration, il devra comporter un mécanisme d'authentification et incorporer un système de déport d'affichage de type VNC.

Le livrable final comportera les développements, le packaging et la documentation (utilisateur, administrateur et de conception) des réalisations

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

- Connaissance de langages de programmation et de script (C, Perl, Python, ...)
- Virtualisation, Cloud
- Environnement Linux, Windows
- Sécurité

Formation :

- Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
- Stage de fin d'études

Qualités requises :

- Ouverture d'esprit et rigueur
- Esprit de synthèse
- Curiosité technique

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1021

Migration Windows 7 vers Windows 10

Description :
L'ANSSI travaille sur différents SI sur lesquels sont déployés des clients Windows. Le poste client de l'utilisateur étant souvent le premier vecteur menant à la compromission d'un SI il est indispensable que celui ci soit sécurisé et maitrisé. Afin de tirer partie des dernières évolutions en matière de sécurité et de gestion de postes clients sous Windows 10, une migration automatisée des postes de travail existants est nécessaire.

Les objectifs du stage sont les suivants:
• Etude des pré-requis d'infrastructure à la migration vers Windows 10 afin de disposer des dernières évolutions en matière de sécurité et de gestion (Virtual Secure Mode, Microsoft Passport et Active Directory, intégration dans SCCM…)
• Etude de l'intégration de Windows 10 dans l'infrastructure existante.
• Mise en place d'une migration automatisée de postes de travail Windows 7 vers Windows 10.
• Création d'un master sécurisé Windows 10 pour le déploiement de nouveaux postes.
Le travail s'effectuera sur une maquette dédiée et le livrable final comportera la documentation des réalisations.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation ou de scripting (C, .NET, Powershell…)
• Connaissance de l'OS Windows
• Connaissance Active Directory.
• Connaissance SCCM et MDT seraient un plus.

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique
• Stage de fin d'études

Qualités requises :

• Ouverture d'esprit et rigueur
• Curiosité et autonomie
• Esprit de synthèse

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1022

Automatisation de la mise en place d'une chaîne de démarrage sécurisée pour serveur

Description :
Du fait de son évolution constante, l'ANSSI opère un nombre croissant de serveurs. Pour chacun de ceux-ci, le démarrage dans un environnement intègre permet une augmentation du niveau de sécurité non négligeable. La mise en place d'une chaîne de démarrage sécurisée devient alors une nécessité. Toutefois, il s'agit d'un processus long et rarement automatisé.

Le but de ce stage est d'étudier le fonctionnement d'une chaîne de démarrage sécurisée intégrant le chiffrement de disque intégral pour des machines de type serveur Linux. Il s'agira de proposer des mécanismes d'automatisation pour la mise en place des différents éléments composant la chaîne. Notamment, l'accent sera placé sur la réalisation pratique. Les différentes tâches du stage viseront à définir des procédures d'automatisation de la mise en place des mécanismes de contrôle d'intégrité sur les composants suivants :
• gestionnaire d'amorçage;
• noyau Linux modifié;
• racine minimaliste du système permettant l'instanciation de conteneurs légers;
• systèmes invités (utilisation d'un HIDS depuis le système minimaliste).
Une seconde partie du stage portera sur l'étude de la mise en place du chiffrement disque intégral. Il s'agira ici d'étudier la distribution et le stockage sécurisé des clés de chiffrement.

Les réalisations seront packagées afin de faciliter leur déploiement et la documentation de conception et d'utilisation sera fournie.

Localisation :
31, quai de Grenelle – 75015 Paris

Durée :
6 à 9 mois

Compétences requises :

• Connaissance de langages de programmation système et de scripting (C, C++, Python, ...)
• Bonnes notions en administration système Linux.
• Bonne connaissance du fonctionnement du noyau Linux et sur les mécanismes de construction d'une distribution.
• Des connaissances cryptographiques de base seront nécessaires.
• Des connaissances du mode de fonctionnement des TPM seraient un plus.

Formation :

• Bac +5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit
• Rigueur
• Capacité à travailler en équipe
• Curiosité

Agence nationale de la sécurité des systèmes d'information

Fiche de stage S1023

Emulation et tests automatisés sur Android

Description :
L'ANSSI, dans le cadre de ses travaux sur Android et de l'amélioration de sa plate-forme d'intégration continue, propose un stage centré sur l'émulation et les tests automatisés sur Android.

Les objectifs de ce stage sont les suivants:
• Emuler l'une des dernières versions d'Android.
• Automatiser l'émulation en question et associer celle-ci aux différents éléments de la plate-forme d'intégration continue de l'ANSSI.
• Proposer des mécanismes permettant d'executer automatiquement une succession de tests sur une ROM Android compilée.
• Documenter les moyens mis en oeuvre pour parvenir à atteindre les objectifs précedents.
Le résultat attendu est constitué d'un outil exécutant une série de test sur une version émulée d'Android et la documentation associée. Cet outil devra être particulièrement modulaire afin de permettre l'ajout facile de nouveaux cas de test.

Localisation :	**Durée :**
31, quai de Grenelle – 75015 Paris	3 à 9 mois

Compétences requises :

• Connaissance d'un langage de programmation (C, JAVA, ...)
• Bonne connaissance de l'environnement GNU/Linux
• Connaissance de base d'Android

Formation :

• Bac +4/5 - Ecole d'ingénieur ou formation universitaire en informatique

Qualités requises :

• Ouverture d'esprit et rigueur
• Autonomie
• Curiosité technique