SYNACKTIV
DIGITAL SECURITY

# Offres de stages en sécurité informatique

## 2018-2019

# Stage Synacktiv : Deep-sea phishing

## Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer au développement du projet existant **Oursin** (http://www.synacktiv.ninja/ressources/synacktiv_oursin_plaquette.pdf). Oursin est une plate-forme de ***spear-phishing*** permettant de mettre en place des **attaques ciblées** de postes clients. Création de scénarios, distribution de charge, **contournement d'antivirus** et **prise de contrôle à distance** font partie de ses fonctionnalités.

Les attaques ciblées sont parmi les clefs de la réussite des intrusions en ***Red Team***. Un mail, une clef USB malveillante sont souvent synonymes de la compromission d'un utilisateur inattentif. La porte est alors ouverte à la **persistance**, au **rebond** et à la **compromission** de masse.

Pour garder une longueur d'avance vis-à-vis des méthodes de défense de plus en plus avancées, les méthodes d'attaque doivent être en constante évolution. En intégrant l'équipe en charge du projet Oursin votre rôle sera de concevoir, améliorer, suggérer de nouveaux composants sur l'outil **Oursin.** À ce titre, vous devrez :

- Imaginer, concevoir, développer et intégrer de nouveaux types de charges utiles et d'**exploits N-Day.**
- Imaginer et mettre en œuvre des méthodes de **contournement des principaux antivirus du marché.**
- Duper les analyses dynamiques de plus en plus courantes et performantes.

Pour intégrer notre équipe, vous devrez également :

- Avoir des bases en développement **Python** et le recul vous permettant de prendre en main un projet existant.
- Être capable de développer et résoudre des problèmes complexes sur un sujet précis : **développer des exploits et des charges utiles innovantes** permettant de prendre le contrôle d'une machine à distance sans éveiller les soupçons des antivirus.
- Travailler en collaboration avec des experts en intrusion expérimentés qui utilisent le projet quotidiennement.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

## Profil recherché

- Forte volonté d'apprendre, de se perfectionner et d'innover sur les **techniques d'attaques des postes de travail.**
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devez avoir une expérience minimale en Python pour contribuer à son développement.
- **Anglais et français indispensables.**
- Poste basé à **Paris**, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com

# Stage Synacktiv : O-ditor

## Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer au développement d'outils de ***post-exploitation***.Dans ce stage, l'expert se basera sur le projet interne **O-ditor**, afin de développer un outil capable d'automatiser la reconnaissance, la découverte de vulnérabilités et les chemins permettant une **escalade de privilèges** sur un système cible déjà compromis (intégralement ou avec des droits restreints). Aujourd'hui, O-ditor est capable de prendre en charge de nombreuses technologies, parmi lesquelles : Microsoft Windows, GNU/Linux, Oracle Solaris, AIX, MySQL, Oracle Database Server, Apache, PHP, OpenSSH, Nagios, etc.

**O-ditor** devra respecter des critères précis :

- Adaptation aux différents systèmes et architectures.
- Discrétion de la phase de reconnaissance et d'extraction d'informations.
- Stabilité et Portabilité.

Ce projet serait développé en plusieurs étapes :

- Fiabilisation des différents modules d'analyse et de collecte existants.
- Conception, développement et intégration de nouveaux modules en fonction des besoins de l'équipe.
- Extension des modules d'analyse afin d'intégrer une recherche des escalades de privilèges.
- Développement d'une intégration avec l'outil **Kraqozorus**.
- Développement d'une intégration avec l'outil **Disconet**.

Il s'agit de :

- De travailler en collaboration avec des consultants en sécurité expérimentés, qui utilisent le projet quotidiennement.
- Conquérir le monde plus rapidement en diminuant le temps passé à lire des fichiers de configuration.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

## Profil recherché

- Forte volonté d'apprendre et de se perfectionner sur les différents systèmes supportés, leurs mécanismes de sécurité et la programmation d'un analyseur de configuration.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement.
- **Anglais et français indispensables.**
- Poste basé à **Paris**, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com

# Stage Synacktiv : Chef de rayon dans un supermarché de bugs

## Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer au développement d'une suite d'outils permettant d'automatiser au maximum **l'audit et le suivi de CMS et frameworks** reconnus (WordPress, Drupal, Laravel, Symfony…) et des modules de tierces parties associés. Le but principal sera de **découvrir de nouvelles vulnérabilités** introduites lors de mises-à-jour ou de les détecter dans le cas de correctifs silencieux.

En intégrant le pôle pentest, votre rôle sera de **gagner une connaissance approfondie du fonctionnement interne** de ces produits vous permettant de concevoir des briques d'outillage facilitant le travail autour de ceux-ci**.** Votre objectif sera de devenir chef de rayon en chef au supermarché de la vulnérabilité. À ce titre, vous devrez :

- Étudier et suivre le code source des frameworks, CMS et bibliothèques PHP répandus, y compris en **analysant des vulnérabilités** publiques existantes.
- **Développer des outils d'exploitation** lors de la découverte de vulnérabilités, y compris les **N-day.**
- Réfléchir à l'utilisation et à l'adaptation **d'outils d'analyse statique** déjà existants.
- **Capitaliser sur vos découvertes** et méthodologies pour aider au travail des auditeurs en boîte noire.
- Travailler en collaboration avec des **experts en intrusion expérimentés** qui réalisent régulièrement ces audits et qui tireront profit de votre travail au quotidien.
- Présenter vos résultats dans des **articles de blog et des conférences**.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

## Profil recherché

- Forte volonté d'apprendre, de se perfectionner et d'innover sur les techniques de **recherche de vulnérabilités** en boîte blanche.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devez avoir une expérience minimale en Python pour contribuer à son développement.
- **Anglais et français indispensables.**
- Poste basé à **Paris**, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis, si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com

# Stage Synacktiv : 0day hunting / reverse-me if you can

## Description du poste

Dans le cadre de différentes missions d'intrusion, les experts sécurité Synacktiv font face à des technologies n'ayant pas fait l'objet de recherches suffisantes. Les outils pour manipuler certains protocoles manquent et les vulnérabilités diffusées publiquement sont souvent de type « unspecified vectors / unspecified impact ».

Synacktiv recherche un stagiaire (H/F) sécurité pour travailler sur la rétro-ingénierie, le matériel et la conception d'outils d'attaques.

Les technologies ciblées seront discutées avant le début du stage. À titre d'exemple, voici une liste de technologies et produits susceptibles d'être étudiés : Citrix, Windows (kernel & userland), Android, iOS, Linux, Cisco IOS, virtualisation, RDP, et d'autres. Il s'agit de :

- Étudier des technologies et des logiciels propriétaires.
- **Développer des outils** permettant de tester la sécurité de ces technologies : canaux de communication, chiffrement, interception, etc.
- **Chercher des vulnérabilités** et de **développer les codes d'exploitation** associés.

Il ne s'agit pas de :

- Rédiger un guide de bonnes pratiques ou de faire une compilation des recherches existantes, même s'il sera attendu une bonne maîtrise des attaques existantes.
- Chercher des vulnérabilités théoriques sans scénarios opérationnels plausibles.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

## Profil recherché

- Forte volonté d'apprendre et de se perfectionner sur les aspects techniques liés à la **rétro-ingénierie**, l'**audit sécurité de code source** et la **recherche de vulnérabilités**.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement.
- Maîtrise des **outils de rétro-ingénierie** comme IDA sur différentes architectures et de l'analyse sécurité de protocoles.
- **Anglais et français indispensables.**
- Poste à pourvoir à **Paris** dans le deuxième arrondissement, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com

# Stage Synacktiv : One fuzzer to rule them all

## Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer au développement de son framework de **fuzzing**.

Le fuzzing est un outil indispensable dans la recherche de vulnérabilités. Il existe aujourd'hui dans l'état de l'art de nombreux moyens pour rendre un fuzzer plus efficace : **génération** et/ou **mutation** de *test-case* intelligente, **couverture de code**, **exécution symbolique**, etc. Cependant, la diversité des cibles et la complexité des logiciels font que les outils existants se révèlent souvent limités et le fuzzing reste aujourd'hui un sujet de recherche ouvert.

Le framework développé par Synacktiv est déjà opérationnel et largement utilisé en interne. Néanmoins plusieurs axes d'améliorations demeurent :

- Amélioration et optimisation des différents composants du framework.
- Développement de **grammaires**.
- Support d'architectures et d'environnements supplémentaires.
- Développement d'outils afin de faciliter la mise en place de campagnes avancées.
- Fuzzer le monde en vue de sa conquête.

Il s'agit de :

- Intégrer de nouvelles fonctionnalités à un outil existant.
- Optimiser les fonctionnalités existantes.
- Travailler sur des cas concrets et bloquants rencontrés par les experts Synacktiv.
- Utiliser la **rétro-ingénierie** afin d'étudier des logiciels *closed-source*.

Il est attendu que le stage débouche sur un CDI d'expert sécurité dans le pôle rétro-ingénierie de Synacktiv.

## Profil recherché

- Forte volonté d'apprendre et se perfectionner en développement bas niveau et en **rétro-ingénierie**.
- Programmation en **C**, la quasi-totalité des composants du framework étant développés en C.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement.
- **Anglais et français indispensables.**
- Poste à pourvoir à **Paris** dans le deuxième arrondissement, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com

# Stage Synacktiv : Offensive Tooling

## Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de rejoindre son **pôle développement**. En plus de créer et maintenir des outils internes au profit des autres départements, le pôle réalise des missions de développement **d'outils d'intrusion** et de sécurité dite offensive. L'expert peut donc être amené à travailler sur des projets de R&D de type : implants et C&C, packer, fuzzer, cassage de mots de passes, spear-phishing, systèmes embarqués, ou autres.

Voici quelques exemples de réalisations précédentes :

- **Kraqozorus** : plateforme de cassage de mots de passes (https://synacktiv.com/ressources/synacktiv_kraqozorus_plaquette.pdf)
- **Oursin** : une plateforme de spear-phishing (https://synacktiv.com/ressources/synacktiv_oursin_plaquette.pdf)
- **Disconet** : un automate collaboratif pour les tests d'intrusions (https://synacktiv.com/ressources/synacktiv_disconet_plaquette.pdf)
- **Houdini** : un système embarqué pour les intrusions physiques (https://synacktiv.com/ressources/synacktiv_houdini_plaquette.pdf)

Ce poste permet de faire **avancer l'état de l'art** de la sécurité offensive tout en ayant la **satisfaction** d'équiper des experts du domaine avec de nouveaux outils d'intrusion !

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

## Profil recherché

- Programmation **Python** et en **C**. Notre suite d'outils internes est principalement programmée en Python et le C reste incontournable pour la programmation système et bas niveau qui en font donc un pré-requis essentiel.
- Expérience en développement en environnement **Linux**.
- Avoir des bases en **sécurité** des systèmes d'information ainsi qu'en **réseaux, cryptographie et systèmes UNIX.**
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques d'intrusion et la sécurité offensive.
- Bonnes compétences rédactionnelles et de communication. **Anglais et français indispensables.**
- Poste basé à **Paris**, métro Grands Boulevards.

## Rémunération

- Stage : **1 500 € brut par mois**. Bonus en fonction des résultats. Puis si passage en CDI : 40 800 € brut par an.

Merci d'envoyer votre demande à apply@synacktiv.com