LA SOCIÉTÉ

MÉTIER

Cogiceo est une société indépendante, spécialisée dans l'audit technique en sécurité informatique. Fondée en 2012 par 2 consultants seniors issues de grandes entreprises françaises, son cœur de métier repose sur l'expertise technique dans le domaine de la sécurité des systèmes d'information et en particulier dans les **tests d'intrusion qui représente 80 % de son chiffre d'affaires.**

OFFRES

Audit

- Test d'intrusion
- Audit de configuration
- Audit d'architecture
- Audit organisationnel et physique
- Audit de code source

RedTeam

- Campagne de phishing
- Social Engineering
- Test d'intrusion physique
- Test d'intrusion de l'exposition Internet
- Test d'intrusion réseau interne

Forensic

- Gestion d'incident
- Digital forensic
- Analyse de malware
- Network tracking

Scan

- ADA : Active Directory Security Analyzer
- LINA : Linux Security Analyzer
- MOBAA : Mobile and Browser Application Audit
- Explorer : Internet Exposure Exploration

Formation

- Sensibilisation C-Level managers et end-users
- Formation sécurité administrateur systèmes et réseaux
- Formation sécurité développeur
- Formation sécurité administrateur AD

ÉQUIPE

Cogiceo est une entreprise à taille humaine composée actuellement de **20 collaborateurs.** Une forte limitation dans la croissance de la structure est clairement affichée afin d'effectuer une formation optimale des collaborateurs et ainsi garantir une excellente qualité de prestation auprès des clients. **Notre équipe est dynamique** et nous souhaitons explicitement nous démarquer des nombreuses SSII sur le marché en prenant le temps de former nos consultants. Nos collaborateurs bénéficient donc d'**importants transferts de compétences et de temps de R&D notables**.

LE STAGE

OBJECTIF

L'objectif global du stage de fin d'études est la formation au métier de consultant en sécurité des systèmes d'information. Dans cet esprit, vous accompagnerez, **50 % de votre temps**, nos équipes de consultants expérimentés sur certaines de leurs missions (principalement sur des **pentests** de systèmes exposés sur Internet puis, selon votre progression, sur des **pentests** de systèmes internes aux SI de nos clients). En parallèle, vous travaillerez **50% de votre temps sur un sujet de recherche académique** (à choisir dans notre catalogue, ou à proposer vous-même).

PROFIL RECHERCHÉ

Le stagiaire doit être en fin d'études de **niveau BAC+5 (École d'Ingénieurs ou Master en Sécurité)** et posséder des bases solides en informatique : réseau, système, développement, etc. De plus, il doit être **passionné par la sécurité informatique** et être capable d'**apprendre rapidement** au contact de consultants expérimentés. Des bases en **Python** seraient fortement appréciées. Les qualités humaines recherchées sont : probité, persévérance, curiosité et autonomie. Des compétences en **exploitation ou administration de systèmes Linux** constitueraient un avantage.

CADRE DU STAGE

- Nombre de postes à pourvoir : 3
- Contrat : convention de stage obligatoire
- Durée du stage : de 5 à 6 mois
- Rémunération : **1300€** par mois
- Avantages : 50 % de la carte de transport, tickets restaurant
- Lieu principal : 28 bis boulevard de Sébastopol - 75004 Paris
- Date d'entrée en poste : au plus tôt
- Horaires : du lundi au vendredi de 9h30 à 18h30 (35h)

DÉBOUCHÉ

Le stage de fin d'études peut déboucher sur une proposition d'**embauche en CDI.**

CANDIDATURE

Pour postuler à ce stage, veuillez **envoyer votre CV** à l'adresse suivante : **stages@cogiceo.com**
Dans votre mail, **vous préciserez le(s) sujet(s) académiques le(s)** plus en adéquation avec vos attentes et les raisons de ce choix, dans l'ordre de préférence. Vous serez recontacté pour un entretien téléphonique avant une éventuelle rencontre dans nos locaux à Paris.

LES SUJETS ACADÉMIQUES 2021

1 - Analyse automatique de la sécurité d'un réseau de serveurs Linux

Pour répondre à un besoin grandissant, Cogiceo a développé un outil d'analyse d'un réseau de serveurs Linux et UNIX. Après s'être familiarisé avec les fonctionnalités déjà implémentées et le développement Shell, le stagiaire pourra travailler sur la partie collecte des données en implémentant de nouvelles fonctionnalités techniques, le support des différents OS, des niveaux plus ou moins profonds de recherches et différents modes opératoires (boîte blanche et boîte grise). La partie analyse des données collectées pourront également être traitées avec la recherche de nouvelles méthodes d'élévation de privilèges et pour établir des chemins de compromissions locaux ainsi qu'au niveau réseau.

2 - Classification automatique de ressources exposées sur internet

La découverte et classification automatique de ressources sont primordiales afin d'analyser la surface d'attaque d'une organisation exposée sur internet. Ces ressources peuvent être ensuite utilisées à des fins de surveillance ou d'intrusion (notamment lors de nos exercices Redteam). Le but du sujet de stage est de mettre en place un algorithme qui à partir d'un ensemble de données (adresses IP, sites internet, service réseaux, enregistrements DNS) détermine automatiquement, si une ressource appartient ou non à l'organisation ciblée. Des connaissances en machine learning et réseaux de neurones seront les bienvenues (mais ne sont pas indispensables).

3 - Audit automatique de la sécurité des domaines Active Directory

Les domaines Active Directory sont omniprésents dans les réseaux d'entreprises. Difficiles à sécuriser, ces domaines représentent souvent la partie la plus vulnérable d'un système d'information.
Pour accompagner ses clients, Cogiceo dispose d'un outil d'analyse du niveau de sécurité des domaines Microsoft. Après s'être familiarisé avec les fonctionnalités déjà implémentées dans l'outil ADAnalyzer, le stagiaire pourra participer à la recherche et l'implémentation de nouvelles fonctionnalités ainsi que l'amélioration globale des performances de l'outil.

4 - Collecte et analyse de leak

Dans le cadre d'audits RedTeam ou de réponse à incident, Cogiceo est régulièrement amené à vérifier si des données appartenant à nos clients ont été piratées puis rendues publiques. Ce sujet de stage vise à améliorer notre capacité dans ce domaine. Dans un premier temps, le stagiaire devra chercher de nouvelles sources d'information susceptibles de contenir des leaks intéressants. Il pourra ensuite développer des codes Python capables de collecter automatiquement des leaks depuis les sources nouvellement identifiées ou depuis d'autres sources bien connues (pastebin, github, etc.). Enfin, il pourra également participer à l'amélioration de l'application Web interne qui nous permet de rechercher et d'analyser ces données récoltées.

5 - FORENSIC

Pour répondre à des missions Forensic de plus en plus fréquentes, Cogiceo a mis en place un outillage centralisé afin d'assister les consultants lors de leurs missions. Les besoins étant souvent variés, la mission du stagiaire consistera à effectuer un état de l'art des indicateurs et des outils existants afin de compléter le panel interne pour permettre des recherches plus approfondies sur un périmètre large ou restreint. Le stagiaire participera ainsi à l'amélioration de notre méthodologie de réponse à incident et à l'industrialisation des analyses liées à ce type de mission.

6 - THREAT INTELLIGENCE

Le stage consiste a effectuer une recherche approfondie et détaillée sur les sujets suivants : acteurs malveillants et groupe APT connus, techniques d'intrusions et outils utilisés par ces acteurs et les malwares les plus connus et les plus répandus sur Internet. Le stagiaire développera également une sonde réseau (honeypot) qui sera déployée sur Internet afin d'obtenir des informations fiables sur les vulnérabilités aujourd'hui exploitées et les adresses IP à l'origine des actions malveillantes. Cette sonde servira également à alimenter notre application interne de réputation.

7 - ANALYSE AUTOMATIQUE D'APPLICATIONS IOS MALVEILLANTES

Cogiceo a développé un outil d'analyse de la sécurité des applications mobiles. Le but du stage consiste à étudier des applications iOS malveillantes afin de déterminer les comportements dangereux. Il sera demandé au stagiaire de développer de nouveaux points de contrôle puis de les intégrer à l'outil déjà existant et enfin de les tester sur un large panel d'applications. Ces points de contrôle concerneront les thématiques de vie privée, de vulnérabilités face aux attaques et de détection de comportement malveillants.

8 - CONTOURNEMENT DE PROTECTION DE PRISE RÉSEAU

Dans le cadre de l'amélioration des outils utilisés lors des missions Red Team, Cogiceo a développé un testeur de NAC. Après s'être familiarisé sur le fonctionnement et le contournement de protection NAC, le stagiaire devra concevoir un boîtier miniaturisé auto-alimenté permettant de tester la présence et la solidité des protections NAC mises en place. Le boîtier devra également être contrôlable depuis une application mobile (sélection des attaques et visualisation des résultats). Une partie du stage sera consacré à la recherche et l'implémentation de nouvelles techniques de contournement des protections NAC (Bruteforce de VLAN, Bruteforce d'adresse MAC, usurpation de certificat, aspiration automatique de certificat sur équipement vulnérable).

9 - CONCEPTION PHYSIQUE ET LOGIQUE D'UN MOUCHARD RÉSEAU

Dans le cadre de l'amélioration des outils utilisés lors des missions Redteam, Cogiceo a développé un mouchard réseau. Après avoir réalisé un état de l'art des solutions existantes, le stagiaire devra concevoir et développer un mouchard réseau miniaturisé permettant le montage automatique de tunnel via une connexion mobile. Ce « Plug and Forget » devra également intégrer un panel d'outils utilisables lors des tests d'intrusion, une interface Wi-Fi, le support du PoE ainsi que la possibilité de stocker les différentes trames émises en broadcast. Une partie du stage sera également consacrée à la sécurisation du mouchard afin de rendre sa détection sur le réseau le plus complexe possible.