LA SOCIÉTÉ

MÉTIER

Cogiceo est une société indépendante, spécialisée dans l'audit de Cybersécurité. Fondée en 2012 par 2 consultants seniors issus de grandes entreprises françaises, son cœur de métier repose sur leur expertise technique dans le domaine de la sécurité des systèmes d'informations et en particulier dans les tests d'intrusion et les audits de cybersécurité qui représentent 70% de son chiffre d'affaires. L'ensemble du système d'information de Cogiceo est situé sur le territoire français.

OFFRES

Audit

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

Red Team

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

Scan

- SEC4AD : Active Directory Security Analyzer
- LINA : Linux Security Analyzer
- MOBAA : Mobile and Browser Application Audit
- Explorer : Internet Exposure Exploration

ÉQUIPE

Cogiceo est une entreprise à taille humaine composée actuellement de 35 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. Cogiceo n'emploie jamais aucun sous-traitant pour ses missions d'audit de sécurité.

LE STAGE

OBJECTIF

L'objectif globale 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'étude de **niveau BAC+5 (École d'Ingénieur 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 : **1500€** par mois
- Avantages : 50 % de la carte de transport, tickets restaurant
- Lieu principal : 95 boulevard de Sébastopol - 75002 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.

SUJETS DE STAGE

ANALYSE DES RISQUES ET PROTECTION DES CLÉS BITLOCKER

Catégories : Pentest, Red Team

Description

Plusieurs solutions de chiffrement de disques reposent sur des mécanismes matériels tel que le TPM pour protéger les données. En particulier, Bitlocker repose sur ce dernier. Cogiceo souhaite accompagner un stagiaire sur l'étude des vecteurs d'attaque pouvant conduire à la compromission des clés de chiffrement Bitlocker. L'état de l'art de cette recherche permettra d'identifier les moyens existants permettant de compromettre ces clés et de mettre en place une méthodologie. Des tests sur des environnements réels seront réalisés afin d'éprouver cette méthodologie.

Objectifs

1. Réaliser un état de l'art et une montée en compétence sur les attaques matérielles en particulier la technologie Bitlocker
2. Identifier les méthodes de compromission des clés de chiffrement Bitlocker
3. Mettre en place une méthodologie afin de réaliser ces attaques
4. Éprouver cette méthodologie dans un environnement réel (un Poste de travail)

MISE EN PLACE D'UNE PLATEFORME DE CTI

Catégories : Développement, OSINT

Description

Dans le cadre de ses missions, COGICEO est amené à évaluer les menaces cyber et notamment d'identifier des comptes valides de ses clients accessibles au travers de leaks publiques. Ce stage vise à évaluer la faisabilité et mettre en place une plateforme interne d'analyse des leaks. De plus, des clients sont régulièrement amenés à subir des fuites d'informations. Une méthodologie de collecte de ces fuites d'informations sera mise en place.

Objectifs

1. Étudier la mise en place et les besoins d'une plateforme de CTI interne
2. Collecter et agréger différentes sources d'informations ou de fuites d'informations
3. Mettre en place une plateforme sécurisé de recherche et de gestion de ces fuites d'informations

ANALYSE DE LA SÉCURITÉ D'APPLICATIONS ANDROID

Catégories : Pentest mobile, Audit automatisé

Description

Cogiceo rencontre dans de nombreux audits des applications mobiles et a développé un outil permettant d'automatiser une partie de l'analyse des applications mobiles Android. Cet outil SaaS est également proposé directement à ses clients. Dans le cadre de l'amélioration de l'outil et de la méthodologie d'audit une revue et une amélioration des contrôles réalisés par l'outil et lors des audit doit être réalisé.

Objectifs

1. Tour d'horizon de la sécurité Android.
2. Création de points de contrôle qui seront intégrés dans notre outil d'analyse.
3. Mise en place d'une sandbox Android.
4. Analyse d'applications malveillantes existantes.

DÉVELOPPEMENT D'UNE CI POUR LA SIMULATION DE VULNÉRABILITÉS ACTIVE DIRECTORY

Catégories : Développement, Pentest

Description

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. Ce projet a pour objectif de concevoir et développer des rôles et scripts Ansible permettant de générer des vulnérabilités spécifiques au sein d'un environnement Active Directory contrôlé. Ces scripts seront notamment utilisés pour tester et valider le bon fonctionnement de l'outil d'analyse Sec4AD ainsi que fournir aux auditeurs un référentiel connu et reproductible pour effectuer des tests pratiques dans leur quotidien.

Objectifs

1. Identifier les configurations associées aux vulnérabilités couramment rencontrées dans des environnements Active Directory.
2. Concevoir des rôles Ansible pour configurer ces vulnérabilités spécifiques (erreurs de permissions, mauvaises configurations, …).
3. Tester et valider ces scripts dans un environnement de laboratoire contrôlé.
4. Documenter les points de contrôles et les résultats attendus pour garantir leur réutilisation et leur maintenance future.

ANALYSE DE CODE ASSISTÉE PAR INTELLIGENCE ARTIFICIELLE

Catégories : Développement, Audit de Code, Pentest

Description

Cogiceo rencontre dans de nombreux audits de code dans le cadre de son activité. Ce stage a pour objectif d'améliorer les méthodologies d'analyse statique du code. Pour cela une évaluation approfondie des méthodes et outils statiques actuels tels que Semgrep sera réalisée. Le stagiaire évaluera ensuite les solutions d'analyse de code automatiques basées sur des LLM (Large Language Model) capables de compléter les analyses traditionnelles par une compréhension contextuelle du code ou une détection de patterns complexes.

Objectifs

1. Réaliser un état de l'art de l'analyse de code et le comparer à la méthodologie actuelle
2. Réaliser un état de l'art de l'analyse de code assistée par LLM
3. Étudier la mise en place de ces solutions dans un environnement local
4. Proposer des améliorations à la méthodologie actuelle d'analyse de code