SERVICE DE CYBER THREAT INTELLIGENCE ET CYBER THREAT HUNTING

CONTACT@WELAN.FR

15 RUE DES HALLES
75001 PARIS
FRANCE

STAGE/ALTERNANCE
6, 12 OU 24 MOIS

Qui sommes-nous ?

WELAN est une société de conseil en cybersécurité qui accompagne les entreprises de toutes tailles désireuses de se protéger contre les menaces numériques croissantes.

Notre équipe est composée d'experts, mais pas que. En effet, nous nous efforçons de mettre en place un environnement favorable à l'apprentissage et au développement professionnel, permettant ainsi aux collaborateurs moins expérimentés de progresser vers le niveau d'expertise attendu au travers de projets d'apprentissage et d'un programme de mentorat.

Quelles que soient nos différences de niveaux, nous partageons tous deux choses : la passion de la cybersécurité et la volonté d'apprendre.

Notre expertise

Alors, pourquoi travailler avec nous ? Notre équipe possède une solide expérience et une expertise technique approfondie dans les domaines de la cybersécurité. Nos services s'articulent autour des 5 piliers suivants :

La **cybersécurité offensive** qui consiste à évaluer ou identifier les faiblesses d'une entreprise au travers de tests d'intrusion, d'audit technique, d'audit de configuration ou d'audit de code.

La **cybersécurité défensive** qui nous amène à accompagner nos clients dans la définition de stratégie de défense ou de roadmap de sécurité, l'intégration d'outils de défense ou la correction de vulnérabilité. Dans le cadre de cette activité, nous avons développé une spécialité dans les projets de sécurisation Active Directory.

La **détection** pour laquelle nous sommes amenés à auditer des prestataires de détection d'incident de sécurité (i.e. SOC), de définir des stratégies de collecte et d'analyse ou encore intégrer des outils de détection et d'analyse (i.e. SIEM).

La **réponse sur incident** qui intervient malheureusement lorsque les mesures de sécurité d'un de nos clients n'ont pas permis de le protéger efficacement. C'est alors que nous procédons à une analyse inforensique de l'incident afin de déterminer le vecteur d'attaque, les actions menées par les attaquants, les portes dérobées installées, les données corrompues ou volées. À l'issue des analyses nous formulons les mesures de corrections et de préventions à mettre en œuvre.

La **conformité** qui permet à nos clients de pérenniser leur niveau de sécurité, de gagner en maturité et de démontrer leur niveau de sécurité à des prospects, à des clients ou à des organismes privés ou publics. Dans ce contexte, nous intervenons en tant qu'auditeurs ou conseiller sur les référentiels SecNumCloud, PDIS, PRIS, PCI DSS, SOC2 ou ISO 27001.

En guise de reconnaissance de notre expertise, quelques-uns de nos consultants ont été qualifiés par l'ANSSI comme auditeurs **SecNumCloud**, **PDIS** et **PRIS**. Ces derniers interviennent, en collaboration avec les centres d'évaluation des prestataires de services, durant les audits de qualification des référentiels précédemment cités.

CONTACT@WELAN.FR

15 RUE DES HALLES
75001 PARIS
FRANCE

STAGE/ALTERNANCE
6, 12 OU 24 MOIS

Description de l'offre

Déploiement, intégration et développement d'outils liés au service de "Cyber Threat Intelligence et de Cyber Threat Hunting".

Le service de CTI&CTH de WELAN a pour objectif de fournir une vision consolidée des menaces, des techniques et des méthodes employées par les attaquants. Cette activité passe par:

- La collecte d'information (en sources ouvertes ou semi-ouvertes)
- L'extraction et l'analyse des marqueurs
- La consolidation des informations collectées
- La diffusion auprès des clients de WELAN
- La recherche de trace de compromission
- L'injection des marqueurs au sein des outils de défense (défense pro-active)

Le développement des outils et des scripts d'analyse se fera en étroite collaboration avec des experts en intrusion et en réponse sur incident.

Profil recherché

Nous recherchons un candidat ayant suivi un parcours spécialisé en sécurité informatique, démontrant une compréhension globale des concepts de sécurité informatique et des cyber attaques.

Ce dernier devrait être fortement orienté vers la technique, doté d'une curiosité naturelle et désireux d'approfondir ses connaissances dans le domaine de la cybersécurité.

Une maîtrise pratique des langages de script tels que Python, Bash ou PowerShell est requise.

Il doit être capable de travailler de manière autonome tout en ayant une bonne aptitude au travail en équipe dans un environnement dynamique.

De plus, d'excellentes compétences en communication écrite et verbale, tant en français qu'en anglais, sont indispensables.