Proximus Luxembourg

Proximus Luxembourg constitue le pilier ICT du Groupe Proximus et fournit des solutions à l'ensemble des sociétés privées et du secteur public avec l'expertise et le support de ses 750 employés répartis sur le site de Bertrange au Grand-Duché.

Son offre comprend notamment des services réseau, système, application, sécurité, mobilité, collaboration, Connectivité et Cloud ; ainsi que des prestations de conseil, ingénierie, support et maintenance.

Fort de son ancrage international dans plusieurs pays et de sa position de leader en Belgique et au Luxembourg, la société a notamment pour objectif de renforcer la présence du Groupe Proximus dans le marché européen des télécoms.

Fort de son engagement depuis plusieurs années avec les Écoles et Universités de la Grande Région et au-delà, Proximus Luxembourg envisage d'accueillir un ou plusieurs stagiaires pour le département de Cyberdéfense de la Société.

Cybersecurity Department

Le département de Cybersécurité de Proximus (anciennement connu sous *Security Audits & Governance Services – SAGS*) est composé de consultants et d'ingénieurs certifiés (GIAC, CISSP, CISM, CRISC, ITIL, ISO27001, ISO27032, ISO27034, ISO31000…) spécialisés en *Information & IT security* en forte présence sur les activités de cybersécurité.

Proximus Luxembourg a développé son département Cyberdéfense autour de quatre pôles.

- **Le pôle SOC** CyberSecurity and Intelligence Operation Center est devenu un atout supplémentaire dans la lutte contre le cybercriminalité grâce à sa capacité à analyser rapidement les menaces à la fois interne et externes.
- **Le pôle Test d'intrusion** avec ses activités de sécurité offensive qui aide les sociétés à détecter les vulnérabilités et failles de sécurités présentent sur leur infrastructure. Les ingénieurs accompagnent ensuite les clients dans les corrections en leur fournissant des recommandations afin et d'améliorer la sécurité.
- **Le pôle Threat Hunting & Incident Response** intervient chez les sociétés qui ont subit une cyberattaque et les aide à éradiquer la menace puis à se protéger contre de nouvelles attaques. Le pôle THIR analyse les méthodes actuellement utilisées par les attaquants afin d'être préparé à intervenir sur tout types d'attaques rencontrés.
- **Le pôle Gouvernance**

Le département est un acteur majeur de la Place pour les prestations de cybersécurité, tests d'intrusion / *ethical hacking* sur les réseaux et les applicatifs et le premier département de pentest certifié ISO 27001. Le Département est également très actif dans la consultance organisationnelle, gouvernance, gestion des risques et conformité légale et règlementaire, en

particulier pour la mise en œuvre et l'audit de systèmes de management de la sécurité de l'information selon la norme ISO/IEC 27001.

Le pôle Test d'Intrusion de Proximus propose les sujets de stage suivants :

Les stages en test d'intrusion amèneront les stagiaires à un travail étroit avec l'équipe de pentest via un support à l'équipe pour le travail au jours le jour avec la création script amélioration des outils de pentest ou de travaux sur le laboratoire de l'équipe. Le stage aura aussi un sujet principal qui pourra être :

- **Pentest in the cloud:** Ce stage s'aligne dans le cadre du développement des activités autour du cloud, de son utilisation pour la réalisation de tests intrusifs ainsi que les méthodologies de pentest à suivre pour tester ce genre d'environnement. Le stagiaire devra prendre en compte et analyser les vulnérabilités et problèmes de configuration pouvant être associés à des services cloud comme par exemple Amazon Web Services (AWS), proposer une méthodologie de test et une stratégie de défense à mettre en place pour limiter l'exposition aux risques. Le stage aura aussi pour but de concevoir une plateforme qui pourra être utilisée afin de simuler différents type d'attaques chez nos clients. L'amélioration de méthodologies ainsi que l'automatisation de certaines activités pentest sur d'autres technologies rentreront aussi dans le cadre de ce stage.

- **Amélioration des outils et méthodologies** : Ce stage a pour but de consolider et améliorer les différentes outils, script et machines qui sont utilisés pour la réalisation des test d'intrusions et des rapports. Il s'agira aussi de créer de machines et des « mallettes » prêts à être utilisés pour les différents types de pentest réaliser dans le service

- **DIY** : Vous souhaitez développer une idée qui lui tient à cœur, venez échanger avec nous pour définir ensemble comment nous pouvons vous accompagner dans la mise en œuvre de votre projet tout en vous permettant de valider votre cursus d'études.

Le pôle Threat Hunting & Incident Response de Proximus propose les sujets de stage suivants :

Automatisation du processus de réponse sur incident : Ce stage s'aligne dans le cadre du développement des activités de réponse sur incident. Il a pour but de permettre au CSIRT de Telindus de gagner en rapiditié lors des investigations forensics. Pour cela, le stagiaire sera amené à automatiser un certains nombres d'actions menées par les équipes de Telindus lors d'investigations forensics. Ce stage s'articulera principalement autour de l'automatisation de l'outil d'analyse mémoire « Volatility ». L'objectif sera de développer une interface graphique qui permettra d'uploader un dump de RAM et d'automatiser l'analyse de celui-ci. Pour cela, certaines commandes devront être lancées automatiquement et les résultats de celles-ci devront être analysés par le programme puis affichés sur l'interface graphique afin de faciliter le parcours et la lecture de ceux-ci.

Développer les processus et outils de Threat Intelligence : Ce stage s'aligne dans le cadre du développement des activités de Threat Hunting et Incident Response et a pour but d'améliorer les techniques permettent de récolter des informations de sécurité et leur donner du sens en fonction des besoins. Afin de mieux se préparer à répondre à de tel incidents de sécurité, il est important de mener une veille technologique intelligente et de trouver et assembler les informations pertinentes concernant les attaquants ou menaces potentielles. Pour cela, la récolte des informations de différentes sources est essentielle mais n'est pas suffisante. En effet, il est important entre autre, de donner tout d'abord un niveau de confiance nécessaire à l'information, de les agréger, de les filtrer, de les organiser et de les représenter de manière adéquate en fonction du besoin. Le stage a pour but d'améliorer les mécanismes de connaissance concernant les menaces et risques afin d'éclairer les décisions concernant la réponse à apporter à ces menaces.

Amélioration d'une plateforme de phishing : Ce stage a pour but de développer et d'intégrer la plateforme de phishing existante de Cybersecurity avec la plateforme Open source « Gophish ». L'équipe de Pentest procède une plateforme de phishing développée en interne (https://paperjam.lu/article/communique-telindus-luxembourg-recompensee) et souhaite continuer à la développer avec de nouvelles fonctionnalité. L'objectif et d'utiliser l'infrastructure existante (Exchange, DNS, server web, script et macros, etc.) afin de la faire interagir avec Gophish afin d'avoir une interface de management simplifié et aussi de pouvoir utiliser certaines nouvelles fonctionnalités.

Le pole SOC de Proximus propose les sujets de stage suivants :

- **Modélisation d'attaques et développement de scenarii de détection :** L'efficacité d'un SOC se mesure par la quantité d'attaques qu'il est capable de détecter. Ce stage s'aligne dans ce cadre via la modélisation d'attaques afin d'en définir les étapes puis le développement d'un scenario de détection pour chaque attaque modélisée. Il s'agit ensuite de les intégrer au SIEM du CSIOC de Proximus Luxembourg afin qu'ils soient ajoutés aux scenarii de détection du service.

- **Amélioration du traitement et de la remontée des logs et optimisation de l'ingestion des serveurs syslog :** Ce stage a pour objectif d'améliorer les chaînes de remontée de logs afin d'augmenter l'efficacité de la détection du CyberSecurity and Intelligence Operation Center. La vitesse de remontée des logs a une influence considérable sur la réaction d'un SOC et donc sur ses capacités à détecter à temps les menaces qui ciblent un système d'information. Le stage consiste donc à améliorer la détection du SOC via l'amélioration de la chaîne de remontée de logs.

- **Amélioration et automatisation du système de reporting :** De façon récurrente, un SOC doit proposer des rapports d'activité. Que ce soit pour des raisons de remise en bonne santé d'un système d'information, d'incident ou de résumé mensuel des activités analysées. Ce stage a pour objectif d'automatiser au maximum la génération des divers types de rapports qui sont produit par le SOC.

Qualités recherchées et attendues

De manière commune à l'ensemble des départements, les stagiaires devront faire preuve :

- d'un esprit startup
- de bonnes bases théoriques (réseau, protocole, système, sécurité),
- d'imagination et d'une vue de l'approche sécuritaire non conventionnelle,
- d'autonomie et de partage des informations et de travail en équipe,
- de bonnes qualités rédactionnelles en français et en anglais,
- d'une bonne présentation
- de facilité d'expression.

Pour les stages à connotation *Ethical Hacking*, capacités en programmation pour l'automatisation de traitements d'informations. Des connaissances en tests intrusifs ne sont pas exigées car elles seront enseignées tout au long du stage. La participation à des sites de challenges type *BrightShadow*, *NewbieContest*, *Rankk*, … étant toutefois considérée comme un avantage. Pour les stages GRC, connaissances sur les systèmes de management des risques et normes phares en sécurité de l'information étant considéré comme un avantage.

Pour le stage du pôle Threat Hunting & Incident Response, des connaissances basiques sur les différentes étapes de réponse à d'incident, le forensics et la threat intelligence ainsi que la participation à des sites de challenges sont considérées aussi comme un avantage.

Pour le stage SOC, une connaissance des évènements de sécurité. Ces éléments pourront être introduits et expliqués tout au long du stage.

Environnement du stage

- Lieu: Bertrange
- Durée: de 4 à 6 mois
- Date de début: à définir

Comment postuler ?

Nous proposons dès à présent plusieurs sujets génériques de stage. Ces sujets assez génériques visent à présenter les grandes orientations envisagées par Proximus Luxembourg S.A. pour des stages à réaliser. Ces sujets pourront être précisés d'un commun accord avec les étudiants et l'Université.

Pour postuler, envoyez votre candidature

- par internet sur https://proximus.csod.com/ats/careersite/search.aspx ou
- email : recrutement@telindus.lu (mettre en CC cybersecurity@telindus.lu)
- par courrier postal : *Proximus Luxembourg S.A. à 18, rue du Puits Romain, L-8070 Bertrange*

Date du document : Octobre 2020
Ces propositions de sujets de stage sont susceptibles d'être modifiées ou adaptées selon les besoins, l'actualité ou d'autres facteurs internes ou externes