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 Services

Le service 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 CyberSecurity and Intelligence Operation Center** (CSIOC) est devenu un atout supplémentaire dans la lutte contre la cybercriminalité grâce à sa capacité à analyser rapidement les menaces à la fois internes 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 (THIR)**, connu publiquement sous le nom de Telindus-CSIRT[1], intervient chez les sociétés qui ont subi 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, Risque et Conformité** propose une gestion de la sécurité de l'entreprise pilotée par le risque, la conformité et un système de management. Pour ce faire, l'entreprise doit avoir une image précise de son exposition et ainsi connaître

[1] *https://www.telindus.lu/fr/cybersecurity-incident-response-team*

ses forces, faiblesses et vulnérabilités. Pour gérer au mieux les ressources disponibles au sein de l'entreprise (humaines, financières, etc.), Telindus propose des solutions de stratégie, de gestion des risques et de conseil, garantissant ainsi un bon niveau de sécurité pour le client.

Cybersecurity Services 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. Ce service 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 notamment Microsoft Azure, 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 types 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 tests 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.

- **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 fonctionnalités. 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.

- **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 Telindus-CSIRT propose les sujets de stage suivants :

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 autres, 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.

Mise en place d'une infrastructure honeypots : Ce stage a pour but de proposer et mettre en place une infrastructure hébergeant des honeypots. Un honeypot est un système intentionnellement vulnérable ayant pour objectif d'attirer les attaquants, ceci afin de pouvoir mieux évaluer l'exposition aux risques liée à l'apparition de nouvelles attaques pouvant ciblées des systèmes / services critiques. L'utilisation des honeypots permet aussi de pouvoir générer de l'intelligence de par l'identification d'éventuels nouveaux TTPs (Tactics, Techniques and Procedures) / IOCs liés à certains groupes d'attaquants, intelligence qui devra être partagées avec les solutions de Threat Intelligence utilisées par le Telindus-CSIRT. L'étudiant devra se renseigner sur l'état de l'art concernant ce genre de solutions et proposer une architecture répondant à la problématique du stage. L'étudiant aura aussi l'occasion de développer ses compétences en reverse engineering, en collaboration avec les membres du Telindus-CSIRT, via l'analyse de certain malware.

Optimisation du traitement des analyses de phishing :

Ce stage a pour objectif de proposer et mettre en place une architecture permettant une optimisation du traitement des analyses concernant des incidents de type phishing, la solution retenue devra s'intégrer avec les différentes technologies déjà mises en place.

Développement de scénarii d'adversary Emulation : Ce stage s'articulera principalement autour d'outils tel que Caldera. L'objectif de ce stage est de développer des scénarii d'adversary emulation qui pourront être rejoué lors de missions clientes

Mise en place d'une solution adversary emulation :

Ce stage a pour objectif de proposer et de mettre en place une solution permettant de réaliser des activités de type « Adversary Emulation ». L'étudiant devra se renseigner sur l'état de l'art concernant ce genre de solutions et proposer une architecture permettant l'exécution de Tactiques, Techniques et Procédures telles que référencées dans la matrice MITRE ATT&CK. La solution retenue devra non seulement prendre en compte l'exécution de ces tests mais devra aussi permettre la génération d'un rapport détaillé indiquant les tests effectués, leurs résultats et les informations nécessaires pour pouvoir améliorer les capacités de détection du Système d'Information mis à l'épreuve.

Il devra être également possible de pouvoir effectuer des gap analysis entre les résultats de différentes sessions d'adversary emulation afin de pouvoir être capable de visualiser concrètement les améliorations.

Mise en place d'une infrastructure d'analyse de fichiers :

Ce stage a pour objectif de mettre en place une infrastructure complète d'analyse automatisée de fichiers et de proposer des axes d'améliorations sur l'infrastructure actuelle. Le process envisagé devra prendre en compte la soumission du fichier via un portail dédié, une analyse statique et dynamique du fichier via l'intégration d'outils spécifiques, la génération et la mise à disposition d'un rapport complet d'analyse via le portail.

Le système de Sandbox devra être constitué de systèmes représentatifs d'un Système d'Information client, la solution retenue devra prendre en compte l'intégration de différentes solutions Antivirus, EDR, XDR opensource et commerciales qui seront choisies en étroite collaboration avec le Telindus-CSIRT.

Le pôle CSIOC de Proximus propose les sujets de stage suivants :

L'automatisation des actions de traitement issue d'une alerte : L'automatisation des actions de traitement liées à une alertes est de nos jours un objectif d'excellence visé par les SOC. Le CSIOC de Proximus Luxembourg dispose depuis peu un SOAR (Security Orchestration, Automation and Response) pour répondre à ce besoin d'automatisation. Le SOAR est basé sur des Playbooks qui permet d'orchestrer et de lancer en automatique un ensemble d'actions lié à une alerte déclenchée par une règle de détection (voir sujet plus bas). Dans ce cadre, le stagiaire devra :

- Créer des Playbooks pour enrichir les informations et les actions suite à :
  - Tentative de brute force
  - Scan réseau
  - Scan de ports
  - Intégration des scénarios avec le playbook principal
- Mettre en place un POC SOAR (intégration complète) :
  - Déploiement d'une instance Cortex interconnectée
  - Déploiement d'une intégration avec un équipement SOAR (ex : PaloAlto EDR, antivirus…)
  - Déploiement de Playbooks associés
  - Rédaction procédure d'installation et configuration

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 aux outils de détection (SIEM/Log management) du CSIOC de Proximus Luxembourg afin qu'ils soient ajoutés aux scenarii de détection du service. En particulier le stagiaire devra se focaliser sur les attaques de type scan et Brute Force et sur le développement de scénarios de machines Learning ELK :

- Comportement inhabituel des utilisateurs
- Comportement inhabituel des machines sur le réseau
- Exploration des différents types de modèles
- Rédaction procédure d'installation et de configuration

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. Le stagiaire devra en autres :

- Rechercher des moyens alternatifs de récupération et de parsing des logs Windows et autres équipements Syslog (ex : NXLOG)
- Mettre en place des agents ELK pour récupération des logs
- Rédiger des procédures installation et de configuration ainsi que de fournir des avis sur les solutions employées

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.

Le pôle GRC de Proximus propose les sujets de stage suivants :

Développer les activités GRC (Gouvernance, Risque et Conformité) de Cybersecurity Services de Telindus :

Dans le cadre de ce stage, le stagiaire sera amené (e) à :

- Analyse de risque :

  - Etudier les méthodologies d'analyses de risques et définir celle qui sera opérée, selon le métier, l'environnement…
  - Concevoir un guide du Risk Manager à destination des consultants définissant par exemple les méthodologies d'analyse de risques applicables selon les objectifs poursuivis, des plans d'entretiens d'analyse de risques, les livrables à disposition, des échelles d'analyse de risques, des glossaires selon les méthodes
  - Participer à des missions d'analyse des risques en interne
  - Collecter, consolider et formaliser le besoin d'appréciation des risques dans les projets
  - Communiquer sur les travaux réalisés auprès de l'équipes GRC pour transmettre l'usage de ces nouveaux documents

- Conformité

  - Contribuer à la mise à jour des référentiels de Cybersecurity Services (Politiques, procédures, templates…)

- Gouvernance :

  - Elaborer un tableau de bord de sécurité selon le référentiel ISO 27004 pour le périmètre Cybersecurity Services de Telindus

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 Telindus-CSIRT, 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 2021
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