Elaboration d’un SIEM Géographique pour une solution de cybersécurité :

La société

Spécialisée dans le développement d'applications dédiées au traitement de l'Information Géographique (IG) comme dans la réalisation de portails d'entreprises et de portails géographiques, GEOMATYS a développé, ces dernières années, une importante activité de services pour le compte d'acteurs majeurs de l'industrie et de la recherche ainsi que pour des collectivités territoriales.

L'entreprise répond, dans ses prestations, à leur souci de mettre en place des plate-formes respectueuses des standards en s'appuyant sur des solutions modulaires et évolutives.

Poussée par une équipe de passionnés, et cultivant une très forte compétence dans la prise en charge de l'IG au travers d'applications Web, Desktop et mobiles, GEOMATYS a mis en place un environnement technique (API, Bibliothèques, Frameworks, Web Services, etc.) complet qui permet d'appréhender l'ensemble des problématiques liées à la spatialisation des Systèmes d'Information (SI).

Lieu du stage :

Montpellier. Site d’Agropolis

Encadrement :

Vincent Heurteaux (CEO) / Robin Gilh (DevOps)

Thème :

Dans le cadre d'un projet visant à réaliser une solution de gestion de théâtre d'opération et de gestion de crise, Geomatys élabore un SIEM (Security Information and Event Management) ayant pour objectif de superviser la sécurité d'un Système d'Information Géographique dédié à la gestion d'un théâtre d'opération civil ou militaire.

Dans le cadre de ce stage vous intégrerez l'équipe en charge du déploiement et de la gestion de l'infrastructure cloud (Docker/Kubernetes) afin d'y déployer un ensemble de solutions de monitoring et de détection d'intrusion. Outre le déploiement d'un IDS (Intrusion Detection System), vous organisez la collecte d'information depuis les différents assets identifiés en réalisant leurs sondes appropriées. La collecte des informations sera réalisée sur la stack ElasticSearch/Logstash/Kibana, déjà opérationnelle au sein de notre infrastructure. L'enjeux majeur de ce stage consistera à représenter la menace via une interface cartographique. Une réflexion sera également menée afin d'intégrer en complément du service de monitoring, des indicateurs de risque issus de travaux de Threat-Intelligence.

Vous serez accompagnés tout au long de votre stage par une équipe constituée d'un administrateur systèmes/Réseaux, d'un RSSI et d'une équipes de développeurs spécialisés dans le traitement et l'exploitation d'Information Géographique.

Compétences souhaitées :

- Gestion des infra cloud (kubernetes / docker)
- Connaissance du langage Java

Contact :

isabelle.pelissier@geomatys.com