Offre n°2024-07775

Ingénieur de recherche : Analysis of cybersecurity logs in hospital environments

Le descriptif de l'offre ci-dessous est en Anglais

Contrat renouvelable : Oui

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Ingénieur scientifique contractuel

Contexte et atouts du poste

This work takes place in the context of a collaboration between the Hospices Civils de Lyon (HCL), Inria Nancy (RESIST Team). and Inria Rennes (CIDRE Team).

Mission confiée

In the recent years, the healthcare sector including hospitals and their OT infrastructure are becoming a target of multiple cyber threats and attacks such as ransomware, data exfiltration, DDoS, etc. The number of these attacks is growing and the safety of patients is becoming critical in such situations. To mitigate such attacks and reduce their impact, some large hospitals are deploying their own SOC (Security Operating Center) or enhancing the detection capabilities of their existing ones. However, hospital IT infrastructures usually contain a large Operational Technology (OT) environment as well as a large number of medical systems, some of them legacy, and IT security staff are also faced with high false positive rates due the complexity of the deployed equipments and their specific requirements (realtime operation, healthcare-specific protocols, sometimes outdated and unsupported software, high availability requirements). Thus, more accurate and precise detection tools are required in such environments to provide a more focused counter-measure to avoid blocking critical operations or disrupting patient care.

The objective of this work is to develop a novel approach for the analysis of security logs in a hospital environment by leveraging Machine Learning (ML) techniques. A large number of logs and alerts is collected daily when monitoring the activities of these networks and their respective deployed equipments. These logs and alerts issued by Intrusion Detection Systems (IDS) and Endpoint Detection and Response (EDR) are mainly stored in SIEM (Splunk). Not all the useful logs are currently collected yet and, for the ones that are collected, they are missing context to distinguish true positive from false positive alerts in order reduce false alarms. This reduction allows the security analyst to focus on a small number of alerts instead of hundreds or thousands per day.

Principales activités

The tasks to be carried by the research engineer are as follows:

- Study of existing attack detection techniques used in hospital and health care environments.
- Analysis of existing logs and the missing ones in order to be able to suitably implement the aforementioned attack detection techniques.
- Development of methods for both cleaning, preprocessing and annotating logs and and alerts. The goal of this task is to build a precise and representative dataset from available logs and alerts provided by the Hospices Civils de Lyon.
- Evaluation of supervised and unsupervised ML techniques for attack detection by using the built dataset.

Compétences

- Cyber security
- Security protocols analysis
- Python programming
- Knowledge about formal methods

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)

- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

From €2765 gross/month depending on qualifications and experience

Informations générales

- **Thème/Domaine :** Réseaux et télécommunications
  Système & réseaux (BAP E)
- **Ville :** Villers lès Nancy
- **Centre Inria :** Centre Inria de l'Université de Lorraine
- **Date de prise de fonction souhaitée :** 2024-10-01
- **Durée de contrat :** 12 mois
- **Date limite pour postuler :** 2024-06-30

Contacts

- **Équipe Inria :** RESIST
- **Recruteur :**
  Lahmadi Abdelkader / abdelkader.lahmadi@loria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.