Offer #2024-07775

Ingénieur de recherche : Analysis of cybersecurity logs in hospital environments

Renewable contract : Yes

Level of qualifications required : Graduate degree or equivalent

Fonction : Temporary scientific engineer

Context

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).

Assignment

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the deployed equipments and their specific requirements (realtime operation, healthcare-specific protocols, sometimes outdated and unsupported software, high availability requirements).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.

Main activities

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.

Skills

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

Benefits package

- 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

Remuneration

From €2765 gross/month depending on qualifications and experience

General Information

- **Theme/Domain :** Networks and Telecommunications
  System & Networks (BAP E)
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2024-10-01
- **Duration of contract :** 12 months
- **Deadline to apply :** 2024-06-30

Contacts

- **Inria Team :** RESIST
- **Recruiter :**
  Lahmadi Abdelkader / abdelkader.lahmadi@loria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.