Research Engineer: Cyber Security Events Format for Security Monitoring and Automation

CentraleSupélec/Inria CIDRE research team

About the research centre

CentraleSupélec is a public institution under ministerial charter, devoted to science and engineering. This charter is shared between the Ministry of Higher Education, Research and Innovation, and the Ministry of Economy, Industry and Digital Technologies. CentraleSupélec was officially established on January 1st, 2015, bringing together two leading engineering schools in France: École Centrale Paris and Supélec. Today we boast multiple campuses across the country: in the Paris region, Metz and Rennes. We have 4200 students and 370 faculty members and researchers, all of whom interact with our global network: three international campuses (China, India and Morocco) and five associated laboratories (Brazil, Canada, The United States and China). We also have successful partnerships with 176 international universities and 140 corporate institutions. Our academic and research excellence is nestled in our firm and fruitful cooperation with large national institutions such as the CNRS, CEA, Inria, ISERM and ONERA. CentraleSupélec is also a founding member of Université Paris-Saclay, the T.I.M.E Network and the Alliance 4Tech, in addition to being strategic partner to ESSEC Business School and holding the presidency of the Groupe École Centrale.

The position will be based in the Rennes Campus of CentraleSupélec, within the CIDRE research team. CIDRE is a joined research group between CentraleSupélec and Inria, focusing on the security of information systems.

Inria is the French national research institute dedicated to digital science and technology. Inria employs 2,600 people. Its 200 research 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.

Context

Security monitoring is one of the main research axes of the CIDRE team. In this context, the team is involved in different research projects in collaboration with industrial, governmental and academic partners. The proposed work will be part of the FUI project entitled SECEF (Security Exchange Format): https://www.secef.net/. The goal of this project is to promote format standardization in cybersecurity. More

Campus de Paris-Saclay (siège)
Plateau de Moulon
3 rue Joliot-Curie
F-91192 Gif-sur-Yvette Cedex
Tél : +33 (0)1 69 85 12 12
Fax : +33 (0)1 69 85 12 34
SIRET : 130 020 761 00016

Campus de Metz
Metz Technopôle
2 rue Edouard Belin
F-57070 Metz
Tél : +33 (0)3 87 76 47 47
Fax : +33 (0)3 87 76 47 00
SIRET : 130 020 761 00040

Campus de Rennes
Avenue de la Boulaie
C.S. 47601
F-35576 Cesson-Sévigné Cedex
Tél : +33 (0)2 99 84 45 00
Fax : +33 (0)2 99 84 45 99
SIRET : 130 020 761 00032

precisely, we want to address the limitation of the IDMEF[1] format and to propose a new RFC for a standard security event exchange format.

In a traditional security monitoring architecture, such events can be raised by security probes (e.g. antivirus, IDS, firewall, etc.) and sent to managers (SIEM) that can correlate them and present enriched information to security operators. If such events correspond to some actual security incident, security operators have to launch appropriate countermeasures to stop the attack and restore the infected systems into a clean state. One of the main challenges and current trend in security monitoring consists in automating the reaction process. To that end, probes have to report useful information to the security automation process, in a structured and standardized format. Moreover, companies and institutions are more and more inclined to exchange information regarding threats, to enhance their detection and reaction capabilities. The security event format developed in the SECEF project should integrate with existing Cyber Threat Intelligence standardization effort, such as STIX[2] or IODEF[3].

In this project, the CIDRE team is involved in:

- studying the state of the art in security event formats;
- specifying a new security event format;
- specifying a transport protocol for this security event format;
- participating in standardisation effort.

On an academic research perspective, we would like to explore how the intrusion detection and reaction approaches we develop in the team could benefit from such a standard security event format. Thus, the recruited research engineer will also be involved in the development of our research prototypes in intrusion detection and reaction systems.

Assignment

The recruited person will be in charge of following the SECEF project for CentraleSupélec. She will collaborate with the industrial and academic partners of the project.

The recruited person will participate to the study of the state of the art. This includes identifying the needs of recent and future security monitoring and automation tools.

She will directly contribute to the specification of the new security event format and to the specification of the corresponding transport protocol. She will be involved in the standardisation effort of the project, including attending IETF meetings.

She will demonstrate the benefits of this format through the study and development of realistic uses cases. To that end, she will contribute to the development of existing and future intrusion detection and response

1 https://tools.ietf.org/html/rfc4765
2 https://oasis-open.github.io/cti-documentation/stix/intro.html
3 https://tools.ietf.org/html/rfc7970

Campus de Paris-Saclay (siège)
Plateau de Moulon
3 rue Joliot-Curie
F-91192 Gif-sur-Yvette Cedex
Tél : +33 (0)1 69 85 12 12
Fax : +33 (0)1 69 85 12 34
SIRET : 130 020 761 00016

Campus de Metz
Metz Technopôle
2 rue Edouard Belin
F-57070 Metz
Tél : +33 (0)3 87 76 47 47
Fax : +33 (0)3 87 76 47 00
SIRET : 130 020 761 00040

Campus de Rennes
Avenue de la Boulaie
C.S. 47601
F-35576 Cesson-Sévigné Cedex
Tél : +33 (0)2 99 84 45 00
Fax : +33 (0)2 99 84 45 99
SIRET : 130 020 761 00032

prototypes of the teams, in close collaboration with PhD and permanent researchers of the team. More generally, she will be involved in the research activity of the team.

She will contribute to the dissemination of the results of the project by presenting the results in scientific and technical conferences, writing articles and developing training materials.

Skills

Candidates will hold a master's degree or a PhD degree in Computer Science or related fields.

- Significative experience in computer security.
- Experience in intrusion detection, security monitoring, incident response or Cyber Threat Intelligence.
- Experience in standardisation process and RFC specification is a plus.
- Ability to read and interpret technical journal and reports.
- Very good skills in English communication and writing.
- Ability to write, understand and debug clean, maintainable software code.
- Skilled in Python, C/C++, JSON, HTTP(S).

General Information

- Theme/Domain: Cyber-Security
- Town/city: Rennes, France
- Starting date: 2021-01-01
- Duration of contract: 21 months (possible extension of 3 months)
- Deadline to apply: 2020-12-30

Salary: 3000-4200€ gross / month, based on experience

This position will 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). Authorization to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of July 3rd, 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.

Contacts

Application documents:

- Resume and over letter
- Recommendation letters
- Copy of the last diploma certificate or equivalent document

The applications should be sent to **Guillaume Hiet** guillaume.hiet@centralesupelec.fr