POST DOC POSITION (24 MONTHS)

DECOR: Detection and optimized correlation for cybersecurity remediations

Starting: April 2024

INTRODUCTION

Cybersecurity technologies have extensively invested at both ends of the operational spectrum, deploying detection tools (SIEM, EDR, NDR, etc.) for generating upstream alerts and leveraging downstream remediation tools (SOAR) capable of executing playbooks. Despite these advancements, the investigative phase remains a vulnerable link in cyber operations. The critical question arises: how can we identify unknown threats that manage to evade detection systems when this pivotal stage lacks reinforcement? While IT managers universally acknowledge the significance of thorough investigation, a mere 3% consider their level of maturity in threat hunting to be adequate. The majority grapple with tool limitations as formidable barriers to effective investigations, compounded by a scarcity of security skills that undermines the robustness of their defense posture.

In this context, the partners of the DeCOR project (Wallix, Malizen, CentraleSupélec) have proposed to develop **new software solutions for reducing the time for detecting and remediating a security incident**.

WALLIX is a cybersecurity software editor, holds the mantle as the European expert in secure access and identity management. In particular, WALLIX develops a solution for accessing and managing IT infrastructures.

Malizen is a company developing a software platform for cyberscurity investigations. Its solution enables to collaborate on the data of IT infrastructures for hunting evidences of a cyber attack.

CentraleSupélec is an engineering school that have an expertise in research in cybersecurity. In particular, the CIDRE team is dedicated to the comprenhension and detection of cyber attacks in IT infrastructures.

In the following, we give the global objectives of the project and we focus on the research questions that the postdoc position will be involved in.

SCIENTIFIC AND TECHNICAL ISSUES

The consortium is supporting research and development efforts on the following operational problems. WALLIX is developing the tool SCAR, that helps to supervize heterogenous devices, such as proprietary firewalls or network sensors. SCAR offers abstractions of rules for configuring quickly new accounts, hosts or sub networks. Malizen is developing a tool for investigating known formats of incident logs or unknown ones with a semi-automated recognition of the log file. The efficiency of the tools is the ability of graphically explore the log, use pivotal informations to explore heterogenous sources, and to use CTI information to enrich the exploration. The tools of WALLIX and Malizen is the heart of the project. They can be used when an incident has been discovered or when an alert comes up of a potential intrusion attemps [1]. We briefly present below the research objectives we intend to develop.

The consortium intends to work on the following challenges:

- Automatic discovery of hosts, LDAP accounts, etc. when scanning a new network/system environment

- Propose a new cartography of the discovered data that can be shared between the tools (supervision tool and investigation tool)

- Device administration (new types of actions on these devices), even with heterogenous technologies

- Network and system remediations when an incident has been discovered
- Generation of recommendations for advising an analyst analyzing an incident [2]

The postdoc position is intended to work at the frontiere of recommender systems and generation of remediations. Indeed, in a complex IT infrastructure, a lot of remediations can be setup, but their impact is difficult to evaluate. For example, the safer decision that can be taken is to switch off all the network connection where a suspicious activity is discovered on a host. If such host has an important role in the infrastructure, the decision may not be taken and alternatives, less intrusive, should be proposed. By collecting information about the network, the hosts and user roles, the running services, adequate solutions could be proposed to an analyst and at the end, technically deployed on the different equipments.

Accurate and reproducible experiments are expected during this project. In particular, it is important to be able to collect datasets of events, during an incident and its remediation. The postdoc candidate will be able to use the infrastructures we develop at CentraleSupélec for this purpose [3]. The prototype of generation of recommendations could be evaluated in this environment, before moving to real tests in infrastructures operated by WALLIX and Malizen.

PROFILE

The applicant must have a PhD thesis in cybersecurity or in a technical field relevant to the subject (network, systems). The applicant should have the ambition to publish the results of the project in international conferences or workshops of the field.

APPLICATION

Deadline: 31/01/2024
Process: Send an email to Jean-François Lalande (jean-francois.lalande@irisa.fr) with a motivation letter, a short CV, and a transcript of academic records.

REFERENCES

[1] Alexandre Dey, « Datascience in support of cybersecurity operations: Adaptable, robust and explainable anomaly detection for security analysts », PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2022.
[2] Dietmar Jannach et al., « Recommender Systems: An Introduction », in: Recommender Systems: An Introduction (Jan. 1, 2010), doi: 10.1017/CBO9780511763113.
[3] Pierre-Victor Besson, Romain Brisse, Helene Orsini, Natan Talon, Jean-François Lalande, et al.. CERBERE: Cybersecurity Exercise for Red and Blue team Entertainment, REproducibility. *CyberHunt 2023 - 6th Annual Workshop on Cyber Threat Intelligence and Hunting*, Dec 2023, Sorrento, Italy.