

Funded by the Erasmus+ Programme of the European Union

**Project title**: Cyber Security Making the energy sector secure.

**Number of students** (minimum 2)**: 2-10**

**Project duration** (1-6 months): 6

**Project frame** (Bachelor/Master, small project): Bachelor, Master, Small Project.

**Background:**

Together with other academic and industrial partners, Aalborg University has taken the lead in developing a National Training Platform for Cyber Security. The platform provides a safe and secure environment, where students and professionals can perform various challenges related to cybers security – basically providing a “hacker lab”, where each team get a machine from which they can attack a number of vulnerable machines and other devices.

The platform is based on a virtualisation environment, and the focus has been on making it easy to use for both students and teachers – in particular, users can access everything in a browser. Through a simple registration process, they get access to a Kali Linux Windows (known for its penetration testing capabilities), from where they can explore their own virtual network including vulnerable machines.

The platform has been accepted for demonstration at Blackhat Europe in December 2019. And it has also been used by important Danish businesses, including the Central Bank of Denmark, companies from the energy sector, and financial businesses.

During 2019, the platform has been successfully extended, making it more stable and extended the number of challenges. We have received a grant for development that runs until April 2021, but we need to think ahead to be able to continue the project.

One direction to explore is to developing training concepts for particular sectors, such as the financial sector and the energy sector. This is what is explored in this project.

**The challenge:**

The project focuses particularly on developing more specific training concepts for the energy sector. The energy sector is interesting, because energy supply is so critical for societies, and because there has been many cyberattacks on this sector in the past: Being able to take down energy supply (or even worse, to incur lasting physical damage) is an extremely dangerous scenario. The questions to be answered are:

* What is the current market for cyber security training, and how could we fit in there?
* What cyber security training is needed in key sectors, including the energy sector?
* How can the training platform be used to meet some of these needs?
* Does it pose additional requirements to the training platform?
* What challenges should be designed in order to do more training within the energy sector?

We hope that the outcome of the project can be both an analysis of the market for cyber security training, a proposition of relevant training concepts that include business and technical aspects, and a set of new technical challenges for the platform.

Key words for business students: Business model canvas, cyber security training concepts, stakeholder analysis.

Key words for technical students: Cyber security, penetration testing, hacker labs, virtualisation environments, docker containers, Kali Linux, user experience.

**The companies:**

The project is carried out between Norlys (a major Danish energy company) and Aalborg University.

**Supervisor:**

The academic supervisors are Ahmet Türkmen and Gian Marco Mennecozzi from Aalborg University. Ahmet is the main responsible for developing the platform, whereas Gian is the main responsible for developing the challenges. From Norlys the supervisor is Kenneth Bjerregaard Jørgensen, who is expert in cyber security.

**Candidate background:**

We are looking for candidates at all levels (B.Sc. and M.Sc.), but will adjust the scope according to the interests and capabilities of students. We are particularly interested in students with knowledge of at least one of the following topics:

* Business IT, Business Informatics and similar (for market analysis and business models)
* Computer Science (for challenges)
* Computer Engineering (for challenges)
* Computer networks (for challenges)
* Knowledge about user interface design or design of computer games (for contributing to the optimal user experience and concept design)

Of course an interest in or curiosity about cyber security is a big advantage!

**References and complementary description:**

Company: [www.norlys.dk](http://www.norlys.dk) (in Danish)

Training platform (open source): <https://github.com/aau-network-security/haaukins>

Try it out: beta.ntp-event.dk (is publicly available when we have enough capacity)

**Screen shots from the current platform:**



