

Management of security (2020-2021)

Lectures

The lectures cover different aspects of *organizing cyber security in an organization*.

There are 10 online or classroom lectures of 3 hours, representing a workload of 30 hours. These lectures must be complemented with an additional workload of about 60 hours of self-study. This represents a total of 90 hours of student workload, or **3 ECTS**.

1. history of cyber attacks, case study
 - historic evolution of cyber attacks
 - case study
 - context for the project
2. know what you are protecting
 - modeling what needs to be protected
 - additional project information
3. decide what you need to do
 - threat modeling
 - risk assessment
 - additional project information
4. pick the right solutions
 - access control
 - multi-level security
 - protecting specific business objectives
5. pick the right solutions (cont'd)
 - network building blocks
 - network architecture patterns
6. pick the right solutions (cont'd)
 - software development
 - certifying software
7. prepare for the inevitable
 - cyber resilience
 - situation awareness
 - operational planning
8. prepare for the inevitable (cont'd)
 - detection capacity
 - threat intelligence
 - resilience instructions on the project
9. stay protected
 - governance and best practices
 - ISO27000
 - NIST CSF
 - CIS CSC
10. stay protected (cont'd)

- NIST security and privacy controls
- CWE mitigations
- secure coding
- education and training
- final instructions on the project

The RMA students will furthermore have **1 ECTS** extra on “*cyber threat intelligence*”.

Project

Objective

The project covers the design and implementation of a security architecture for a specific (fictitious) organization. The specifics of this organization will be presented to the students during one of the lectures and will be described in a separate document.

The project represents a workload of 60 hours for the students, corresponding with **2 ECTS**.

The results of the project are to be documented in a written report, that:

- must be sent as a **PDF**
- to w.mees@cylab.be
- before **31may21 EOB**

Evaluation

The evaluation consists of two parts:

- daily work (weight 1/3): written project report
- exam (weight 2/3): oral exam about the theory, with application to the project

Communication

Slides

The slides are made available at <https://cylab.be/> under “Resources - Slides”. Always verify you have the latest version.

Course notes

It is strongly recommended to acquire the reference course book “Pragmatic cyber-security”. This book is available from Amazon at <https://www.amazon.fr/dp/B08M88KT25>.

Mailing list

General information about the course, as well as last minute changes, will be communicated using the “Management of security” mailing list. You can subscribe to this mailing list at <https://cylab.be/maillinglists>.