ACEN

INTERNSHIP

Attack Detect Defend

Description of the assignment

ACEN is a leading provider of comprehensive cybersecurity solutions in Belgium. We offer organizations of all sizes and across all industries the protection they need against cyber threats. Our team of experts brings extensive experience and expertise, delivering tailored solutions that address each customer's specific requirements. We are committed to staying up to date with the latest threats and technologies, ensuring that our clients remain one step ahead of potential security breaches.

The objective of this assignment is to expose interns to both offensive (red team) and defensive (blue team) security practices. The project is divided into several phases, with the details and execution largely determined by the interns themselves.

The assignment consists of the following phases:

1 Environment

a) Setting up a laboratory environment.
b) Researching and deploying a SIEM solution.

2 Attack

a) Researching different attack techniques and available tools.
b) Executing the previously researched attack chain.

3 Investigate

a) Researching existing forensic artifacts and available tools.
b) Conducting a forensic investigation

4 Report

a) Preparing a management summary of the simulated attack from both the offensive and defensive perspectives.
b) Creating an incident timeline.

5 Harden

a) Investigating potential mitigations for the attack chain.
b) Implementing hardening measures and verifying their effectiveness in preventing the attack.

6 Retrospective

a) To be defined by the interns throughout the course of the assignment.

Objective

Minimum Requirements

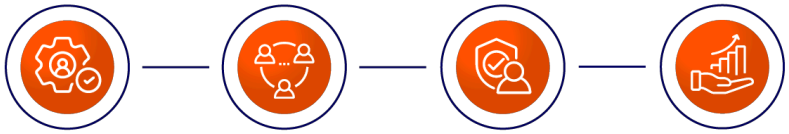
Students are expected to deliver at least the following:

- A successful attack against a laboratory environment.
- A minimum incident report covering the simulated attack.
- Documentation of both the methodology and the results for each phase.

Methodology

ACEN applies agile project methodologies such as Scrum to its projects, and this assignment is no exception. These methodologies place the quality of software solutions at their core. This is achieved by dividing the project into phases in close collaboration with the interns and by maintaining intensive communication both within and outside the project team. Continuous communication is an inherent aspect of agile methodologies and consequently results in thorough internship guidance and support.

Profile



Expertise **Collaboration** **Integrity** **Innovation**

Contact details

Contact person	Cindy Van den Hoecke	**cindy.vandenhoecke@acen.eu**