Secura Internships
2020 - 2021

Secura Internships 2020 - 2021

Version 2020-2021_1.4
24-11-2020

CONTENTS

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Netherlands

Karspeldreef 8
1101 CJ AMSTERDAM
Netherlands

T +31 (0)88 888 31 00
E jobs@secura.com
W secura.com

1 INTRODUCTION

Secura is a Centre of Excellence in Digital Security. For this reason, research & development and knowledge sharing (including presentations and publications) are of essential importance to the organisation. Secura is looking for graduates who want to conduct their final internship assignment with Secura.

Secura actively looks for young talent with a BSc/MSc background and preferably a technical focus (i.e. computer science, information science, cyber security, electronics, physics etc.). We believe that young talent combined with the experience we already have leads to a better and safer digital future.

This document provides several ideas for internships. We welcome your unique take on these ideas or other proposals for internships. We are more than willing to see what is possible and what is not.

The document structures the available internship projects by grouping them to the existing service lines existing within Secura. Considering this, the projects are split between the Security Assessment, Security Certification, Product Development and Advisory and Audit categories.

- The projects within the Security Assessment categories address technical issues and are intended to be executed by students with background and interest in technical penetration testing assignments in a wide variety of topics.
- The projects within Security Certifications are a combination of literature research (for collecting and refining security requirements from various available publications) and technical security validation assessment (for demonstrating the efficiency and possible limitations of the developed standardized methodologies). Additionally, these projects can be supplemented with the development of service descriptions documentation and training/workshop material
- The projects within Product Development are aimed at enhancing and developing tools to be used further by Secura or to be externally released. These projects are designed mostly for students with software development background and programming experience.
- The projects within Advisory and Audit are aimed at creating enhanced methodologies for performing audits, focused on the validation of processes and procedures in place. At the same time, the security awareness programs development is a goal of these project as well.

All our internships are in English unless stated otherwise.

2 SECURITY ASSESSMENT

2.1 Pentesting report automation

Project Overview			
Goal:	Realize tool plugins or scripts that process tool output to automate parts of pentesting reports.		
Location:	Eindhoven	Timeframe:	6 months
Complexity:	Medium	Team:	Security Specialists
Category:	Software development	Supervisor:	Ben / Geert / Mari
Student Attributes			
Education:	WO, MSc preferably, in computer science or the cyber security field		

Technical skills:	• Proven affinity with security and pentesting
	• Proven experience with software development
	  ◦ Languages: Python, Java/C are a pre
	  ◦ Git workflows
	  ◦ Creation of Unit Tests and documentation
	• Affinity with LaTeX is a pre		

Soft skills:	• Structured and organized way of working, good writing skills • Ability to work well in an international team environment • Good communication skills, self-organization		

Project Description

Within this internship we ask your support to build various tools and scripts that aid pentesters in creating reports more efficiently. While most serious pentests and vulnerability assessments cannot be automated, certain parts that are included in almost every report can.

In this internship you will work with highly skilled ethical hackers and you will identify what needs there are within the pentesting team for automation and propose solutions and implementations. This might include for example Burp Suite plugins, Python scripts to parse Nessus-output or scripts that perform static checks on mobile applications. You will learn a lot about specific tools that ethical hackers use. The focus of this internship is heavily on the actual implementation of the tools.

We foresee the following steps:

1) Identify the needs of the pentesters in what parts of the workflow can be automated.
2) Discuss with the management on the solution options and roadmap
3) Create an architecture, processes flows and requirements (use cases) document for the identified workflows that will be automated
4) Support in technical development of a part of this solution (and learn a lot about vulnerabilities)
5) Host internal sessions to the team on the new way of working

2.2 Pentesting of healthcare security infrastructure

Project Overview			
Goal:	Pentest an integrated security infrastructure aimed at transfer and storage of healthcare data		
Location:	Eindhoven/Amsterdam	Timeframe:	5 months
Complexity:	Medium	Team:	Security Specialists
Category:	Penetration testing	Supervisor:	Christiaan
Student Attributes			
Education:	WO, MSc preferably, in computer science or the cyber security field		
Technical skills:	• Proven affinity with security and pentesting • Theoretical knowledge of cryptography • Affinity with LaTeX is a pre		
Soft skills:	• Structured and organized way of working, good writing skills • Ability to work well in an international team environment • Good communication skills, self-organization		

Project Description

Secura is currently involved in a large scale EU level project called **ASCLEPIOS** (https://www.asclepios-project.eu/). The objective of ASCLEPIOS is the development of an infrastructure aimed at secure transfer and storage of patient healthcare data. In this sense, novel encryption mechanisms are deployed in the infrastructure, such as SSE (Symmetric Searchable Encryption) or ABE (Attribute Based Encryption). **A critical element of the project is the testing and validation of the created architecture and infrastructure**. This will allow the project partners to determine and fix possible security vulnerabilities associated with the infrastructure. Also in turn the project pilots based on the above mentioned infrastructure will need to be tested and validated.

Within this project, the student will work under the supervision of one of Secura's experienced technical experts involved in the ASCLEPIOS project. Under this supervision, the student will get in direct contact with the other ASCLEPIOS consortium partners in order to obtain the necessary information for the execution of the penetration testing activities. The following project phases are envisioned:

- P1. Initial understanding of the project and background of ASCLEPIOS architecture
- P2. Alignment with the ASCLEPIOS consortium partners for obtaining sufficient information on the architecture, current state of the developer infrastructure and current state of the created pilots
- P3. Definition of test plan, focused on both the infrastructure alone, as well as the applicable pilot demonstrators
- P4. Conducting the tests in the test plan and recording the results
- P5. Alignment with the partners in ASCLEPIOS for the smooth dissemination and discussion of the testing findings.

2.3 Exploitability automation

Project Overview			
Goal:	Automatically determine the degree of exploitability, given bugs in a program.		
Location:	Eindhoven/Amsterdam	Timeframe:	6 months
Complexity:	High	Team:	Security Specialists
Category:	Binary analysis	Supervisor:	Sjors
Student Attributes			
Education:	HBO, WO, MSc preferably, in computer science or the cyber security field		
Technical skills:	• Proven affinity with low level code, e.g. ARM assembly • Proven affinity with programming in Python • Experience with binary exploitation is a pre • Background knowledge of binary analysis is a pre		
Soft skills:	• Structured and organized way of working • Ability to work well in an international team environment • Good communication skills		

Project Description

Secura is currently involved in a large scale EU level project called **SANCUS** (https://www.sancus-project.eu/). The objective of SANCUS is to create and test a framework which can automatically judge the security of an IoT device. One part of this assessment is the automatic detection of vulnerabilities in compiled software. Through binary analysis techniques such as fuzzing and symbolic execution it is possible to find bugs in code, but it requires another step of analysis to determine whether such a bug is exploitable and thus a vulnerability.

During this internship you will work together with Secura in the SANCUS project to take this next step, and build on top of existing tooling which detects bugs. We foresee the following steps:

1) Orientation phase of binary analysis and -exploitation, as well as the context of the internship.
2) Coordination with the SANCUS consortium partners and design of a possible solution.
3) Implementation of the design, along with a possible/probable redesign.
4) Testing of one or multiple implementations.

2.4 Firmware extraction automation

Project Overview			
Goal:	Automatically extract and virtualize the firmware of an IoT device for further analysis.		
Location:	Eindhoven/Amsterdam	Timeframe:	6 months
Complexity:	Medium	Team:	Security Specialists
Category:	Software development	Supervisor:	Jim
Student Attributes			
Education:	HBO/WO in computer science or the cyber security field		
Technical skills:	• Proven affinity with Linux OS fundamentals • Proven affinity with programming in Python • Experience with embedded Linux is a pre • Experience with virtualization in QEMU is a pre		
Soft skills:	• Structured and organized way of working • Ability to work well in an international team environment • Good communication skills		

Project Description

Secura is currently involved in a large scale EU level project called **SANCUS** (https://www.sancus-project.eu/). The objective of SANCUS is to create and test a framework which can automatically judge the security of an IoT device. One part of the project is to create the tool for analysing embedded Linux firmware for common vulnerabilities. The firmware to be analysed is commonly running on an IoT device (IP camera, router etc). Oftentimes, the operating system components are not available in a format that is suitable for direct analysis. In these cases, the operating system must be extracted from a firmware update, or security researchers have to reside to extracting a raw memory dump from the embedded device's persistent memory.

A previous internship initiated the development of a tool that aims to deploy a tailored virtual environment in which the embedded operating system can interactively be loaded and analysed. Development of this tool must be continued to improve its applicability and to increase the range of devices it supports. To know the required improvements, a study must be performed by the student on the performance of the current tool.

The second part of the internship concerns improvement of automated firmware extraction capabilities of this tool. A brief study of commonly used file systems and compression methods must be performed by the student. The goal is to reliably support the most common firmware images found in today's consumer IoT devices such as squashFS and various forms of UBI (FS).

At the end of the internship, a clear overview on the current state of the project must be presented, including a benchmark of the tool on various common consumer IoT firmwares.

During this internship you will work together with Secura in the SANCUS project to take this next step, and build on top of existing tooling which detects bugs. We foresee the following steps:

5) Orientation phase of automated firmware extraction.
6) Coordination with the SANCUS consortium partners and design of a possible solution.
7) Implementation of the design, along with a possible/probable redesign.
8) Testing of one or multiple implementations.

2.5 Issue tracker integration

Project Overview			
Goal:	Define and implement functionality to upload issue tracker integration.		
Location:	Amsterdam	Timeframe:	6 months
Complexity:	Medium	Team:	Security Specialists / IT
Category:	Software development	Supervisor:	Robert / Ben

Student Attributes

Education:	WO, MSc preferably, in computer science or the cyber security field
Technical skills:	• Proven affinity with security and pentesting • Proven experience with software development (Python/Django) • Any experience on systems like TOPDesk/JIRA is a pre
Soft skills:	• Structured and organized way of working, good writing skills • Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

Within this internship we ask your support to build various steps to move towards an issue tracker integration system with our client.

We foresee the following steps:

1) Create an architecture and requirements (use cases) document
2) Identify how to produce our latex reports in json format (including steps on how to reproduce etc) (from our reporting tooling)
3) Identify smart ways group certain findings
4) Create integration possibilities with common issue tracker APIs like TOPdesk or JIRA
5) Integrate this functionality to our customer portal

Please note that additional encryption mechanism will be in place, especially when sending data via APIs to our clients (about findings!).

2.6 Unit test design and implementation for hackers

Project Overview			
Goal:	Define and implement functionality to unit test Secura's LaTeX report template		
Location:	Eindhoven	Timeframe:	6 months
Complexity:	Medium	Team:	Security Specialists
Category:	Software development / Testing	Supervisor:	Ben / Geert

Student Attributes

Education: HBO, WO, MSc preferably, in computer science or the cyber security field

Technical skills:

- Proven experience with software development
- Proven affinity with software testing
- Any experience with LaTeX is a pre

Soft skills:

- Structured and organized way of working, good writing skills
- Ability to work well in an international team environment
- Good communication skills, self-organization

Project Description

Secura's LaTeX reporting templates are the basis for the delivery of all reports from the Security Assessment team (team with ethical hackers). These templates include a large amount of automation for the pentesters and are under constant development to implement new standards and findings. All pentesters work from this core!

With the increased development speed, there is a need for a unit-testing framework as this template is a software product. This means that new developments can break existing functionality unintentionally. This leads to longer software development cycles and more bugs then necessary. Within this internship we ask your support to build various steps to move towards having fully integrated unit tests in a CI/CD pipeline. Hence we are looking for a software developer with a passion for security!

We foresee the following steps:

1) Create an architecture and requirements (use cases) document
2) Identify how our LaTeX reports are produced and what parts are sensible to test
3) Develop unit testing categories and tests that can easily be expanded. These should be based on solved issues.
4) Integrate with the CI/CD pipeline in GitLab, so every commit is tested before a push to master is allowed.
5) Document all relevant tests and create a description how new tests can be added in an easy fashion.

The goal of this internship is to set everything up with a fair amount of unit tests. The goal is not to simple create as many unit tests as possible. We are really looking for somebody who can think creatively about how to do this smartly.

2.7 A Burp plugin to Automate API Security Testing

Project Overview			
Goal:	Building a pentest solution to automate API security testing by extending burp functionalities.		
Location:	Amsterdam	Timeframe:	6 months
Complexity:	Medium	Team:	Security Specialists / IT
Category:	Software Development	Supervisor:	To be determined

Student Attributes	
Education:	MSc in computer science or the cyber security field.
Technical skills:	• Proven affinity with security and pentesting • Proven experience with software development (Java/Python) • Familiarity with Burp and its plugins is a plus
Soft skills:	• Structured and organized way of working, good writing skills • Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

Burp has proven to be an essential tool in the workflow of any pentester. Although it provides a substantial automation with multiple features it lacks in several cases the fine-tuning that is required for properly testing the cutting edge APIs provided by some clients.

Secura believes that the future of API pentesting is about to change drastically. We are teaming up with a University with the goal to set-up an open-source automated API pentest tool. In the collaboration we aim to build the bridge between the first draft of an academic tool and the current situation at clients. By automating a part of our current API pentest at one of our clients, we can learn how to do this in more detail in practice and figure out how to build this future most effective. For this project you will actually work with one of our clients, which is a large well-known global party operating at the forefront of security and fighting off constant attacks to their teams.

The goal of this internship is to create a pentest solution to automate specific API security testing by extending Burp functionalities to be able to handle these cases, and more specifically the following steps are identified:

- Parsing of OpenAPI/Swagger specifications to identify endpoints.
- Custom filtering from already existing traffic to identify endpoints in the case where a specification is not available.
- A range of features to allow tweaking the connection details for each case (e.g peer tokens, basic auth, consecutive requests, etc).
- Building a methodology of testing endpoints based on their details (this is the most complex part!)
- Providing features to help the pentester with PoC in reports.

What you need:

With the increased volume in APIs, It is essential to cover the most probable scenarios during a test, therefore it is required by the candidate to be self-driven and able to research for the optimal solution in each case. You must have a basic understanding of the concepts of security and penetration testing,

especially in regard to APIs. A proven experience in software development is essential as the main goal is to create a full proof solution up to the industrial standards.

Screening:
You will get the chance to work directly with one of our Clients, gaining access to confidential and sensitive projects, therefore, you should be prepared to pass a screening process both from Secura and the client.

What you get:
You get to be working alongside security experts from our Team, who will be able to assist and guide you throughout the entire duration of the internship. It is a unique opportunity to gain experience and skills in development of security cutting edge solutions.

2.8 Custom internship

Project Overview			
Goal:	Custom internship		
Location:	Amsterdam/ Eindhoven	Timeframe:	1-12 months
Complexity:	To be determined	Team:	Security Specialists / IT
Category:	To be determined	Supervisor:	To be determined
Student Attributes			
Education:	BSc/MSc preferably, in computer science or the cyber security field		
Technical skills:	• To be determined		
Soft skills:	• Structured and organized way of working, good writing skills • Ability to work well in an international team environment • Good communication skills, self-organization		

Project Description

For highly skilled and independent interns we can create custom internships for their final thesis projects. We do this for short term 1 month OS3 master research projects as well as for full final thesis projects of 6-9 months of duration for both BSc and MSc students.
We aim for projects close to our core with a strong technical component. We welcome your ideas and are open to discuss these.

3 SECURITY CERTIFICATIONS SERVICES

4 SECURITY ADVISORY, AUDIT, TRAINING AND AWARENESS

4.1 Security Incident Response & Security Awareness

Project Overview			
Goal:	Research - Security Incident Response & Security Awareness		
Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium	Team:	Security Specialists, Advisors, Trainers
Category:	Awareness	Supervisor:	Floris/ Erwin

Student Attributes	
Education:	• Bsc. or MSc level of education in relevant domain
Technical skills:	• Ability to read, interpret and analyze researches • Writing and presenting • Knowledge about information security (focus on people/ process)
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

To what extent do organisations link IT incident response procedures with security awareness programs?

1. Research large security incidents and how they are handled.
2. Research theory and best practices regarding security incident response.
3. Research the implementation effectiveness of documented (security) policies, processes and controls and gain insight on most successful implementations and how this is related to security awareness (education).
4. Investigate different approaches of creating security awareness (mass communication, training, gamification, e-learning etc.) à What is most successful approach? Define criteria and develop example material.
5. Conclude research by defining the relation between security awareness and incident response?
6. Based on your research, define what is the most effective process of incident response process and follow up by describing a concrete advice.
    a. How to define what an incident is?
    b. How to assess (potential) impact?
    c. How to communicate?
    d. How to process, follow up and close the incident?
    e. How to related to incident to improving security awareness?
    f. How will security incidents be reduced by this?

Literature

- Farahmand, F., Navathe, S. B., Enslow, P. H., & Sharp, G. P. (2003, September). Managing vulnerabilities of information systems to security incidents. In *Proceedings of the 5th international conference on Electronic commerce* (pp. 348-354). ACM.
- Hammer, J. M., Ge, R., Burke, C. D., & Hubbard, C. (2015). *U.S. Patent No. 9,027,121*. Washington, DC: U.S. Patent and Trademark Office.
- Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, *25*(7), 522-538.

- Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, *12*(5), 16-26.
- Schultz Jr, E. E., Brown, D. S., & Longstaff, T. A. (1990). *Responding to computer security incidents: Guidelines for incident handling* (No. UCRL-ID-104689). Lawrence Livermore National Lab., CA (USA).
- Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, *18*(1), 26-42.
- West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (csirts)* (No. CMU/SEI-2003-HB-002). Carnegie-mellon univ pittsburgh pa software engineering inst.
- Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.
- Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, *24*(6), 448-459.
- Ishiguro, M., Tanaka, H., Matsuura, K., & Murase, I. (2006, October). The effect of information security incidents on corporate values in the Japanese stock market. In *International Workshop on the Economics of Securing the Information Infrastructure (WESII)*.

4.2 Security Awareness – Develop eLearning modules

Project Overview			
Goal:	Support in development of eLearning modules in Secura's Security Awareness Learning Management System.		
Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium	Team:	Security Specialists, Advisors, Trainers
Category:	Awareness	Supervisor:	TBD

Student Attributes	
Education:	• Bsc. or MSc level of education in relevant domain
Technical skills:	• Ability to write, present • Knowledge about information security (focus on people/ process) • Pro: experience in developing training/ educational materials
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

Secura offers a comprehensive set of Training Courses & Awareness services. Our awareness program is called SAFE: Security Awareness For Everyone. Training and Awareness provides a foundation for a sound security culture within an organisation.

Within this program, Secura provides eLearning to its customers. As eLearning is in continues development we look for internships related to developing new and improving existing eLearning modules with focus on: content, animations and questionnaires.

4.3 Security Awareness - How to make security top of mind?

Project Overview			
Goal:	Develop relevant fun factors like a game or other materials in order to increase the fun factor in Security Awareness and help customers to bring this more top of mind.		
Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium	Team:	Security Specialists, Advisors, Trainers
Category:	Awareness	Supervisor:	TBD

Student Attributes	
Education:	• Bsc. or MSc level of education in relevant domain
Technical skills:	• Ability to read, interpret and analyze researches • Writing and presenting • Knowledge about information security (focus on people/ process)
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

To be discussed in detail and based on interest of the intern.

4.4 OT Cyber Security – OT Site Assessment

Project Overview	
Goal:	The main goal of the project is to improve and standardize our way of assessing cyber risks in OT/ICS environments. Secura offers its clients an OT site assessment. The main goals of these assessments are: - Analyse possible cyber related threats to a specific site/plant/factory. - Assess the related risks, their likelihood and possible impact. - Present the findings. - Advise on improvement, based on risk classification. The current methodology is based on experience, knowledge of IT and OT and good practice. We are seeking to improve our methodology on various aspects. The biggest challenge is the assessment of the risks, because traditional probabilistic risk assessment does not really work well in OT/ICS. Therefore, a more formal, standardised methodology is needed for ranking OT related risks and their impact. The first step of creating the methodology would be to analyse the existing classical risk assessment methodologies and all applicable standards relevant for OT/ICS environments. In general two types of methodologies shall be created: - The detailed risk assessment methodology; - The high-level risk assessment methodology. Created methodologies shall include the repository of potential risks/theats that might be applicable for OT/ICS environments. Moreover, on top of 20 weeks reserved for the creation of risk assessment methodologies, the internship might be extended to support Secura with creating templates relevant for current projects portfolio.

Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks + 4 weeks (support with templates)
Complexity:	Medium/High. Thesis	Team:	Security Specialists, Consultants
Category:	Advisory	Supervisor:	Anna Prudnikova

Student Attributes	
Education:	• Bsc. or MSc level of education in relevant domain
Technical skills:	• Strong preference: already familiar with industrial automation / OT environments. The ideal candidate would already have an MBO/HBO education in process automation • Knowledge of information security (and preferably risk assessment methodologies). • Ability to develop frameworks and templates • Plus: knowledge of and experience with IOT (and IIOT).
General skills:	• Analytical skills, ability to read, interpret and analyse research, standards • Writing and presenting skills
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

We determine various parts for further developing as part of one internship.
These parts are (Project output):

1. Standardize OT Risk Assessment Methodology in 2 ways: full risk assessment methodology and high-level risk assessment methodology
2. Subgoal: Creation of a repository of potential risks/threats applicable for OT/ICS environments.
3. Subgoal: Standardization of the way of working. Assure repeatability
4. Subgoal: Standardizing the findings, improving templates.

To be discussed in detail and based on interest of the intern.

5 SECURITY PRODUCT DEVELOPMENT

5.1 Secura File Exchange – End-to-end encryption

Project Overview			
Goal:	Secura File Exchange – add end-to-end encryption		
Location:	Amsterdam	Timeframe:	3-6 months
Complexity:	Medium	Team size:	1-3
Category:	Product Development	Supervisor:	Robert Meppelink
Student Attributes			
Education:	BSc/MSc		
Technical skills:	Python, Front-end programming, Encryption protocols. Django is a plus.		
Soft skills:	Team player, interact with internal stakeholders		

Project Description

As a security company, Secura has to exchange confidential data with her customers. This has to be done in a secure, but user friendly way. Within this internship, you will help adding a new module to the Secura File Exchange platform.

The goal of this assignment is to add end-to-end (E2E) encryption to the Secura File Exchange platform. E2E encryption means that sender uses its browser to encrypts the information before it is sent to the server. The receiver decrypts the information on-the-fly in the browser. In this scheme, the information is kept confidential, even if the server is/becomes untrusted.

In this assignment you will investigate different methods for E2E encryption (e.g. use the signal protocol), select the best one, and implement the solution in the platform.

You will work in a small team and have the ability to make a difference. We work with modern technologies (Django and python) and frameworks. Obviously, secure coding is an important part of the development design.

5.2 Secura Customer Portal

Project Overview			
Goal:	Secura Customer Portal		
Location:	Amsterdam	Timeframe:	2-6 months
Complexity:	Medium	Team size:	1-3
Category:	Product Development	Supervisor:	Robert Meppelink
Student Attributes			
Education:	BSc/MSc		
Technical skills:	Python &Django		
Soft skills:	Team player, interact with internal stakeholders		

Project Description

As a security company, Secura has to exchange confidential data with her customers. This has to be done in a secure, yet user friendly way. Within this internship, you will help adding modules to the Secura Customer Portal in order to facilitate the day-to-day interaction with our customers.

The platform will contain modules that aligns with Secura's project flow, from the intake up to the delivery and follow-up of the project. All customer interaction, including planning and project progress information is managed via this portal. This also includes coupling the portal with our internal ERP system.

Another important pillar is reporting on issues found during our security assessments. We aim to create a dashboard with the issues for a specific customer, linked to our knowledge base on possible mitigations or resolutions.

You will work in a small team and have the ability to make a difference. We work with modern technologies (Django and python) and frameworks. Obviously, secure coding is an important part of the development design.

5.3 SOC Test Tool

Project Overview			
Goal:	SOC Test tool		
Location:	Amsterdam	Timeframe:	2-6 months
Complexity:	Medium	Team size:	1-3
Category:	Product Development	Supervisor:	Robert Meppelink
Student Attributes			
Education:	BSc/MSc		
Technical skills:	Python, Django, offensive security skills		
Soft skills:	Team player, interact with internal stakeholders		

Project Description

Many organizations struggle with their SOC/SIEM security monitoring and detection systems. Initially, they generate a large number of alerts, or none at all. After fine tuning the use cases, it becomes more easy to manage and the number of false positives decreases. However, it is difficult to know if the systems are seeing the events you want to know about.

When a security operations center (SOC) does not alert you to any security events, it could be there is no security event taking place. It could also mean the SOC is malfunctioning or certain attacks are outside the detection capabilities. The Secura PurpleBox provides a test platform to continuously test and verify the functioning of the SOC and provides the trust that real events will not go unnoticed.

Within this internship you help expanding the Secura PurpleBox: a modular and secure test platform that can execute a number of simulated attacks, modeled after the MITRE ATT&CK Matrix for Enterprise.

You will work in a small team and have the ability to make a difference. We work with modern technologies (Django and python) and frameworks. Obviously, secure coding is an important part of the development design.