Secura Internships
2020

Secura Internships 2020
Eefke Ruisbroek
Version 2020_2.4
29-05-2020

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Netherlands

Karspeldreef 8
1101 CJ AMSTERDAM
Netherlands

T +31 (0)40 23 77 990
E jobs@secura.com
W secura.com

CONTENTS

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 / Robin / 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 Automated IoT testing environment

Project Overview			
Goal:	Development of an environment (software executing on an hardware platform) for deploying an automated set of tests on IoT products		
Location:	Eindhoven	Timeframe:	3-4 months
Complexity:	Medium	Team:	Security Specialists
Category:	Technical	Supervisor:	Jim/Robin

Student Attributes	
Education:	• BSc level of education in a technical field of study (Computer Science, Engineering, Security)
Technical skills:	• Technical knowledge for performing a security assessment of a product, based on derived requirements • Affinity with programming and embedded software
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

Within the IoT security group, there is a need for fast and efficient assessments, especially in the domain of consumer IoT products. The reason for that is that the high number of incoming consumer IoT products does not allow for intensive security testing on each of them. A method based on which a conclusion regarding the security of a product can be taken quickly is essential in handling such a big volume of products. Automation is at the base of creating such an efficient testing method.

Secura, in collaboration with external partners, has already defined a testing baseline for IoT products. Examples of assessed areas include:

- Password security
- Role separation and authorization
- Protection of open ports and interfaces
- Protection of data in transfer and at rest
- Software updates security
- Existing vulnerabilities scan, etc.

Some of these tests can be executed in an automated fashion, while some others require human contact and interpretation. The focus for this internship is in the set of tests that can be performed fully in an automated fashion. The objectives of the internship are as follows:

- Selection of generic test criteria which can be performed in a remote manner, on currently unknown targets.
- Analysis of the selected criteria, defining the concrete way in which these can be executed remotely.
- Programming the automated tests, using the Python programming language.
- Embedding the automated testing software into a hardware platform, which can be connected to the product under test, effectively achieving a portable test environment. Consider generic signals such as Wi-Fi or BTLE to be prime targets.
- Creating the possibility of generating automated test reports, exporting these to LaTeX which at minimal include the results and conclusions of the conducted tests.

2.3 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 / Robin
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!).

2.4 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 / Robin / 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.

2.5 Pen-testing of various container orchestration platforms

Project Overview			
Goal:	Penetration testing of a		
Location:	Eindhoven	Timeframe:	3-5 months
Complexity:	Medium	Team:	Security Specialists
Category:	Penetration testing / Infrastructure specialists	Supervisor:	Dave / Tom
Student Attributes			
Education:	WO, MSc preferably, in computer science or the cyber security field		
Technical skills:	• Proven affinity with security and pentesting • Hacker mind set to create creative abuse cases • Comfortable with the *nix command line		
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			

In just a few years, container technology has dramatically changed the way software organizations build, ship, and maintain applications. Container platforms, led by the seemingly ubiquitous Docker, are now being used to package applications so that they can access a specific set of resources on a physical or virtual host's operating system.

These application packages, or better called microservices are broken up into various discrete services that are separately packaged in (Docker) containers. The benefit, especially for organizations that adhere to continuous integration and continuous delivery (CI/CD) practices, is that containers are scalable and ephemeral—instances of applications or services, hosted in containers, come and go as demanded by need. This is where various container orchestration frameworks come in.

For example, Kubernetes, which is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.

Additionally Kubernetes has become synonymous with cloud native container orchestration. An example of a cloud Azure Kubernetes Service (AKS).

Within this internship we aim to work together to standardize and optimize infrastructure investigations / Penetration tests for common container orchestration solutions. Like, Kubernetes, Apache Mesos and Docker Swarm.

First we will provide you with in-depth insight into how we perform crystal box infrastructure investigations and penetration tests by our consultants. Then you will research how to adapt these investigations to include container orchestration technologies .

As an additional goal of the project, the improved container orchestration assesment methodology will also be mapped to Cis baselines, an internationally recognized framework used for assessing the IT security for a scala of container orhcestration solutions.

Within this internship we ask you to do the following:

- Create a testing guide that can be used by our specialists to ease crystal box infrastructure assessments and penetration tests.
- Use baseline tools to perform to assess the IT security status of the solutions against CIS Baselines.
- Discuss and standardize which tests/functionality to check with our experts

Your focus in this project will be:

- Performing a vulnerability assessment in order to determine the most feasible attacks applicable to the architecture
- Conducting penetration testing in line with the determined vulnerabilities
- Clearly reporting the results of the conducted testing
- Providing feedback in addressing the discovered issues in an efficient manner

2.6 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

3.1 IoT Security Pilot(s) based on standardized assessment framework

Project Overview			
Goal:	Practical piloting of the IoT assessment framework		
Location:	Amsterdam/Eindhoven	Timeframe:	3-5 months
Complexity:	Medium	Team:	Security Specialists
Category:	Technical	Supervisor:	Razvan/Robin

Student Attributes	
Education:	• MSc level of education in a technical field of study (Computer Science, Engineering, Security)
Technical skills:	• Ability to read, interpret and analyze standards and regulations • Technical knowledge for performing a security assessment of a product, based on derived requirements
Soft skills:	• Ability to work well in an international team environment • Good communication skills, self-organization

Project Description

The security of IoT products and services is an area in which Secura intends to establish itself as one of the key players. Regulations related to the automotive domain are currently on a very low maturity level or not exiting at all. This is why Secura invested time into the research of the relevant standards, frameworks and guidelines addressing security requirements relevant for the domain of (consumer) IoT.

As a result of this research, an extensive security assessment framework has been created, addressing the security of IoT products from a holistic point of view. Considered categories of requirements include hardware and software security, operating system, interfaces, connectivity to web, cloud or mobile applications, as well as procedural requirements related to the privacy, supply chain or development process.

In practice, within the domain of IoT products manufacturing we see a lot of fragmentation, also due to the lack of laws and regulations. As a result of this fragmentation, different manufacturers have different views and priorities concerning the security validation of their products. Due to this, Secura would like to create various types of IoT testing services, which would fit the wishes and interests of its different customers.

More specifically, the following assessment packages, based on the Secura IoT Testing Framework, need to be defined and matured:

- Quick and efficient IoT testing assessment, focused on small subset of critical tests
- Baseline security assessment
- Enhanced security assessment
- Advanced security assessment

The scope of these different packages will include a growing number of security tests, starting with a small (and preferably automated) baseline, and going all the way to an extensive assessment for the “Advanced” security assessment package.

Within this proposed project, the following elements are in scope:

- Clear definition of the contents of different assessment packages, considering the amount and type of security tests included
- Maturing the defined services, by adding clear testing guidance and metrics, required documentation and evidence and automating the execution as much as possible
- Piloting the defined services at least once, in order to demonstrate their efficient execution, and generate good quality example reports which can be used further as demos to interested customers.

4 SECURITY ADVISORY, AUDIT, TRAINING AND AWARENESS

4.1 Information Security – Cyber Security Health Check

Project Overview	
Goal:	Secura has developed a (self) assessment / security health check using the Secura Cyber Security Framework [SCSF] (combining some ISO 27k standards, ISO 31000 and the latest version of NIST Cyber Security Framework). The approach is based upon determining the inherent cyber security risk of an organisation combined with the critical assets. Followed up by an analysis of available and implemented controls using the SCSF. The SCSF is built upon areas of interest further defined in objectives and intended to determine: 1. Relevance for the key inherent risks; 2. Categorizing the controls in People, Process, Organization and Technology; 3. Maturity level at objective setting level. The goal of this internship is to develop this model further into 4 levels: 1. **Cyber Security Health Check - Self-Assessment** (online version creating a basic overview and scoring) 2. **Cyber Security Health Check – Basic workshop**, based upon a kick-off plus an investigation using interviews and a workshop to determine highest priorities) 3. **Cyber Security Health Check - Baseline measurement**, which is an extensive assessment of multiple days, stakeholders focussed on granular maturity scoring. 4. **Cyber Security Health Check - Full scope audit** – where evidence checking by an independent auditor is involved at the detailed control level rather than the objective level used in 1 – 3. Especially for assignment at larger organizations and where governance is involved. Objective of the Cyber Security Health Check is: • It helps customers to simply explain where our customers are in addressing cyber security • It defines what domains require attention • It helps customers to spend their budget where it is most needed. • It gives insights compared to other organisations

Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium	Team:	Security Specialists, Advisors, Trainers
Category:	Advisory	Supervisor:	Erwin Jansen + selected SME

Student Attributes	
Education:	• Bsc. or MSc level of education in relevant domain
Technical skills:	• Ability to read, interpret and analyze researches, standards • Writing and presenting

	• Knowledge about information security • Ability to develop online surveys, scorings and dashboards.
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. One or more can be covered into one internship. These parts are:

1. Description of the 4 levels of Cyber Security Health Check, process steps, fact sheet, etc.
2. Further Development of the Self-Assessment, questions, basic scoring and online dashboard
3. Further Development of the Secura Cyber Security Framework including method for measuring related to applicable standards.
4. Execution of the Cyber Security Health Check - Self-Assessment Online or Basic.
5. Supporting the execution of the Cyber Security Health Check- Baseline Measurement or Full scope audit

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

4.2 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)*.

4.3 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.

4.4 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.

4.5 Audit/ Audit Project - To be determined

Project Overview			
Goal:	Secura delivers many advisory and audit projects that can be combined with internships/ graduation projects. For more information and custom program, please contact us.		
Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium	Team:	Security Specialists, Advisors, Trainers
Category:	Audit	Supervisor:	Ruud Kerssens/ Mario Sleegers

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.
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.

4.6 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 doesn't really work well in OT/ICS. Therefore, a more formal, standardised methodology is needed for ranking OT related risks and their impact.

Location:	Amsterdam/Eindhoven	Timeframe:	20 weeks
Complexity:	Medium/High. Thesis	Team:	Security Specialists, Advisors, Trainers
Category:	Advisory	Supervisor:	Erwin Jansen + selected SME

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
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):

4. Standardize OT Risk Assessment Methodology.
5. Subgoal: Standardization of the way of working. Assure repeatability
6. 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.