Internship EY ITRA FSO
Information for internship and thesis students
# TABLE OF CONTENTS

I. Introduction .................................................................................................................. 3

II. What we offer ............................................................................................................... 4
   1. Thesis Support ........................................................................................................... 4
   2. Internships ............................................................................................................... 4
   3. International students ............................................................................................. 5

III. What we expect .......................................................................................................... 6

IV. How to apply .............................................................................................................. 7

V. Contact ....................................................................................................................... 8

VI. 2015 – 2016 Thesis and Internship Topics ............................................................. 9
   1. Legal Watch for Information Security ................................................................. 10
   2. The Wondrous World of Security Awareness .................................................... 11
   3. Enforcing and controlling secure development within organizations ............ 12
   4. Malware creation framework .............................................................................. 13
   5. Creation covert communication channels framework ...................................... 14
   6. Extension hacking challenges framework and creation of workshops .......... 15
   7. Threat intelligence framework ........................................................................... 16
   8. Alignment of penetration testing methodologies with industry standards .... 17
   9. Penetration testing approach for web application frameworks ..................... 18
  10. Penetration testing workshop .............................................................................. 19
  11. SharePointify the planning sheet ......................................................................... 20
  12. Brand monitoring framework ............................................................................. 21
  13. Malware testbed .................................................................................................... 22
  14. Internal and External marketing campaign ....................................................... 23
  15. Study on the merits, the security impact and the rollout of Data Loss Prevention . 24
I. Introduction

The purpose of this document is to explain the services EY IT Risk & Assurance FSO offers to potential thesis and internship students.

EY IT Risk & Assurance (ITRA) FSO has been offering internships to Belgian and international students since 2006. Interns and thesis students have become our main pool of recruitment, as the profiles we look for are so rarely found via other recruitment channels. We aim at last year students (Bachelor as well as Master) in the following subject fields: Computer Science, Informatics, Informatics Management, Telecommunication, Multimedia Management, Commercial Science, Applied Economics, Economics and Finance. However, as an innovative recruiter EY is always open to people with non-standard profiles, whom we would like to encourage applying for internships or theses as well.

Students with international interests, supported by their college or university’s Erasmus program, may be interested in our internship opportunities in Spain (Barcelona) or Ireland (Dublin).
II. What we offer

Most undergraduate and postgraduate programs require their students to either write a thesis, or run an internship. EY ITRA FSO offers services for both.

1. Thesis Support

We support Professional Bachelor theses and Master theses. The biggest advantage of working as a consultant is the fact that you thoroughly get to study many different environments and their workings. We can offer you our client connections for your surveys, our software, hardware and lab environment for testing purposes, and our extensive experience on the subject matter you study.

After an initial interview to determine our mutual interests, we assign a subject matter expert who functions as your primary contact. He or she will either help you with the questions you have, or provide the persons and resources you need. We can also proof-read draft versions of your thesis. It is important to note that we do not teach you basic writing or planning skills: it is your responsibility to deliver your thesis timely and in line with the college or university requirements.

Our fields of expertise for thesis support are the following: Information Security, Business Continuity & Disaster Recovery, IT Audit and Risk Management. Further in this document you will find a list of topics we currently offer. This is however not an exhaustive list, and any topic you propose that is within our line of expertise will be taken into consideration. We strongly encourage people with out-of-the-box ideas, especially in the field of Information Security, to apply.

2. Internships

We support internships for Professional Bachelor students and Master students. Internship duration is minimum 8 weeks in Belgium, minimum 12 weeks abroad.

In our profession, we work with confidential data that belongs to high-profile clients. Therefore we do not allow internship students to perform direct client work. Instead, they work project-based: they study a topic of their choice or build a tool for us to use. You work in our office in Brussels and on our infrastructure. Students with part-time jobs or other commitments can be allowed to work from home or one of our smaller offices (Ghent, Antwerp, Liège) if their project allows it, and after approval from their university or college.

Our fields of expertise for internships are the following: Information Security, Data Analytics, IT Audit, Business Continuity & Disaster Recovery, and Risk Management. Further in this document you will find a list of topics we currently offer. This is however not an exhaustive list, and any topic you propose that is within our line of expertise will be taken into consideration. We strongly encourage people with out-of-the-box ideas, especially in the field of Information Security, to apply.

Internship students do not earn a fixed wage, but transport costs are reimbursed and you receive a daily lunch allowance.
Every year, EY organizes an international conference in the United States for its most prestigious internship students. Every student with an internship of at least 8 weeks stands a chance to be selected. Because generally the quality of our Belgian ITRA FSO internships is quite high, your chances to be selected are quite high as well. More information can be obtained via the contact details below.

3. International students

International students are offered the same as our normal thesis or internship students. EY has extensive experience in employing people from foreign countries, and can help you with the practicalities. We however do not provide administrative support, and expect your country’s Erasmus program or other international exchange program to take care of this. Upon your arrival in Belgium, even before you start your internship, one of the ITRA FSO team members will be assigned as your “godfather” or “godmother”, to help you with your settlement in Belgium.
III. What we expect

We expect enthusiasm, motivation, creative thinking and independence. Especially the latter is very important to us. Because we are highly committed to client work, we are not often in the EY office, and therefore not always there to hold your hand. Our internship students need the confidence to ask for us if they need us. We expect that you lead your project, and we guide you. If you ask for help, we will do whatever it takes to get you back on track, but we cannot do your research for you.

Our experience taught us that we offer ideal thesis support and internships for mature students with a high level of independence that are committed to their studies. Many of our ex-interns and thesis students now work for us, and are willing to talk about their experiences on request.

The legend goes that EY interns are expected to work evenings and weekends. This is however not the case: you do not work more than 8 hours a day (and only 6 on Fridays). If throughout the course of your project you realize it will not be completed timely, we help you in finding a solution. We prefer half-finished quality projects over completed but low-quality projects. Of course we will never send you home: if you want to spend 16 hours a day on your projects, you may do so using our environment and our equipment. You will receive a laptop that you can take home in the evenings.
IV. How to apply

Students interested in thesis support can contact us for an interview, and if we have a mutual interest a primary contact will be assigned. This person will further provide answers to your questions and will fulfill your requests to the best of his or her efforts. Thesis support can be performed under contract or without contract. Under contract you receive a company laptop and the possibility to work in our secure environment. Without contract you are not allowed to work in the EY office, nor do you receive a laptop, lunch allowance, or transport cost reimbursement. We always work with non-disclosure agreements.

Students interested in internships can contact us for an interview, and if we have a mutual interest are offered a contract. You receive an EY laptop, lunch allowance and transport cost reimbursement, and are expected to work full-time in our Brussels office. Working from home or from one of our local offices can be negotiated if your project allows it.

Students interested in international internships can contact us for an interview. If we have a mutual interest, we organize a second interview with the internship coordinator in the country of your interest (currently you have a choice between Spain and Ireland). If you pass this second interview successfully, matters are handled further directly between you and the internship coordinator of your country of destination. You are then subject to the local regulations for internship students, however the Belgian office can provide support upon request.
V. Contact

Please direct all your questions to the EY ITRA FSO Belgium Internship Coordinator. You can find the contact details below.

<table>
<thead>
<tr>
<th>Dieter Vandenbroeck</th>
</tr>
</thead>
<tbody>
<tr>
<td>EY ITRA FSO</td>
</tr>
<tr>
<td>De Kleetlaan 2</td>
</tr>
<tr>
<td>1831 Diegem</td>
</tr>
<tr>
<td>Belgium</td>
</tr>
<tr>
<td>Office: 0032 (0)2 775 60 54</td>
</tr>
<tr>
<td>Mobile: 0032 (0) 494 90 70 02</td>
</tr>
<tr>
<td>E-mail: <a href="mailto:dieter.vandenbroeck@be.ey.com">dieter.vandenbroeck@be.ey.com</a></td>
</tr>
<tr>
<td>Website: <a href="http://www.ey.com/be">www.ey.com/be</a></td>
</tr>
</tbody>
</table>
VI. 2015 - 2016 Thesis and Internship Topics

We would like to stress that this is not an exhaustive list. We strongly encourage people with out-of-the-box ideas in our areas of expertise to apply. Our areas of expertise are: Information Security (Attack & Penetration, Secure Development, Forensics, Security Awareness, Social Engineering, Physical Intrusion, ISO2700X Compliance, Privacy, etc.), Data Analytics (Data Mining, Data Cleansing, Data Leakage Prevention, SAS, etc.), ERP Systems (SAP and other), IT Audit, Business Continuity & Disaster Recovery, Risk Management and Vulnerability Management.

Examples of past internships and theses are:

- Building a database for vulnerability management (Internship – Katholieke Hogeschool Kempen);
- Building a password cracking tool (Internship – Artesis Hogeschool Antwerpen);
- DNS tunneling techniques (Thesis – Rijksuniversiteit Gent);
- DNS tunneling techniques (Internship – Hogeschool Gent/Katholieke Hogeschool Kempen);
- Setting up an international Attack & Penetration wiki (Internship – Lessius Mechelen);
- Raising security awareness in different company types (Internship – Lessius Mechelen);
- Impact of EU Data Protection Regulation on the Belgian financial sector (Thesis – H.U. Brussel);
- Competitor analysis of IT Advisory services (Thesis – H.U. Brussel);
- Mobile attack & penetration (Internship – Universiteit Hasselt);
- Performing a penetration test on an IPv6 network (Internship – Katholieke Hogeschool Sint-Lieven);
- Building a CTF framework (Internship – Katholieke Hogeschool Leuven);
- Security implications of the Internet of Things (Internship – Katholieke Universiteit Leuven)
- Creation Social Engineering toolkit and development supporting Command and Control server (Internship – AP Antwerpen)

Current open topics are described in the following sections.
1. Legal Watch for Information Security

Organizations based in Belgium must comply with a plethora of laws and regulations, not only on a local level but also in a European context. A violation of information security legislations can have grave consequences, ranging from reputational damage and a small investigation by the regulator to enormous financial penalties.

We are looking for a student who can skim through existing and upcoming regulations and apply them to the context of information and IT security. This should result in an overview of applicable (parts of) laws and regulations on a local, Belgian, European, or even global level, applicable to organizations in the financial sector.

Once completed, we would like our student to translate what is said in the law to concrete statements on how an organization can implement certain measures to legally comply.

This topic is suitable for 1 student in the format of an on-site internship.

**Required skills:** We require someone with excellent English (all our deliverables are in English), Microsoft Word, interest or background in law, interest or background in information security.

**Optional:** Knowledge of legislation specific to the financial sector (Belgium and Europe).

**Goals:**

- Extensive understanding of the current and upcoming laws and regulations on the different levels related to information and IT security.
- A complete overview of laws and regulations on different levels applicable to organizations in the financial sector.
- An extensive document stating how an organization can implement certain measures to legally comply.
- [If the opportunity arises and time allows it] Organize a presentation or workshop for all EY colleagues to inform on all upcoming regulations, separated for all levels. Create a clear presentation with sufficient notes so that this can also be used in other offices.
2. The Wondrous World of Security Awareness

On a regular basis, EY gives security awareness trainings to employees in all sorts of organizations. This can range from explaining what a phishing attack is to an HR responsible, to providing training in secure development to a developer. Every year our training material is updated to remain abreast of the latest developments in information security.

We are looking for a student with excellent research skills and an extensive personal network with a focus on IT / information security who can give us an overview of interesting hacks, attacks, or developments in information security that have occurred in the last 12 months. For example: phishing is no longer fashionable and has been replaced by vishing, spear phishing, or other techniques. What are these concepts and how do they work? Can you give examples of attacks that occurred and their consequences? We noticed that attacks on NFC become more and more common, and scams via QR codes – how do these work and how can we protect against it?

The result of the internship should be a folder of interesting information around security hacks, scams, and other evil things that occurred in the recent years.

This topic is suitable for 1 student in the format of an on-site internship or a written thesis.

Required skills: We require someone with top-notch adept if IT/information security who has the network to remain abreast of the latest developments, and excellent English (all our deliverables are in English).

Optional: Experience in or knowledge of attacks specific to the financial sector.

Goals:

- Extensive understanding and a complete overview of recent and current attacks.
- Extensive understanding and an overview of attacks most relevant to the financial sector.
- Documentation on past attacks, success rates, and other relevant information.
- Some detailed use cases of specific financial institutes (required information will be provided) to be used internally as examples
- [If time allows it] Create an information campaign to be used in financial institutes to inform IT personnel and business people on the attack landscape.
- [If the opportunity arises and time allows it] Organize a presentation or workshop for all EY colleagues to describe the different concepts, with a clear focus on the advantages and disadvantages of the different concepts. Create a clear presentation with sufficient notes so that this can also be used in other offices.
3. Enforcing and controlling secure development within organizations

Companies these days already face the responsibility to be compliant with numerous security measures. Although companies are becoming increasingly aware of their security responsibilities, a proactive approach in developing applications in a secure manner is lacking. This topic is research-based, and should result in the description of a manner of enforcing and controlling secure development by companies.

This topic is suitable for 1 student in the format of a written thesis; a part-time on-site internship is required.

Required skills: We require someone with excellent programming skills and a basic knowledge of software development lifecycle management (though experience is not required).

Goals:

- Extensive understanding of principles of secure development.
- Extensively describe the principles of secure development in the written paper in an understandable way, both for people with IT technical background and people with a business background.
- Describe the advantages of secure development being enforced within organizations.
- Describe possible disadvantages (especially on the business side) of enforcing secure development principles.
- Design a model that allows an organization to enforce and especially control secure development.
- [If the opportunity arises and time allows it] Apply the theoretical model to a real-life organization as a test, and improve the model based on the results.
4. Malware creation framework

As described in the topic ‘Malware analysis: an automated approach’, malware is an increasingly complex and everyday problem. While analyzing the general network security – and more specifically the anti-malware security- implementations found at clients, it’s important to have some malware at hand.

There exists a wide variety of malware samples (also specifically for the banking sector) and techniques (including evasion / fingerprinting techniques). There is currently however no clear overview of all of these samples and techniques, and there is no easy way of creating new samples using new techniques.

This topic is suitable for 1 student in the format of an on-site internship.

Required skills: we require someone with good knowledge of malware and malware infection concepts. Furthermore, a good knowledge of Linux, Windows and networking is preferred to be able to perform the practical implementation.

Goals:

- Create and set up a malware creation framework, based on existing samples and different techniques.
- Create documentation on the different samples and techniques used.
- Create documentation on the sample creation process.
- [If time allows it] Create an easy to use interface where malware samples can be created.
5. Creation covert communication channels framework

During security tests performed on an internal network, the problem of enforced communication policies is often encountered. These policies are created and enforced to protect the internal network and data found there from malicious attackers. Because the EY security team often performs assessments from the viewpoint of a malicious attacker (during APT / red team tests), it’s necessary to evade these security communication policies.

One of the solutions for this problem is covert communication channels: these are communication channels that are not allowed as such but are still possible to use on the secured network. The key challenges for these channels are to remain hidden and to offer sufficient bandwidth. Communication channels over DNS are well known and multiple implementations exist; however, this method is rather easy to detect the unusually high amount of DNS requests, while the channel offers relatively low bandwidth.

This topic is suitable for 1 or 2 student(s) in the format of an on-site internship.

Required skills: we require someone with experience in programming and protocols.

Optional: Knowledge of malware and/or evasion techniques is a plus.

Goals:

- Work out multiple covert communication channels that are suited for a typical business environment.
- Create a working set-up for each channel.
- Clearly describe the attributes of each channel (bandwidth, possible detection patterns, relation to ‘real-world traffic’, etc.).
- Create a framework containing all this information.
6. Extension hacking challenges framework and creation of workshops

EY has created a proprietary hacking challenges framework, which will be used during the proprietary internal training and external workshops. This framework is developed to be used with a wide variety of challenges and challenge mechanisms, each targeted at specific skills and at a specific target (including services, DMZ, offline crypto challenges, etc.).

We are looking for an internship student to create a wide array of hacking challenges in multiple categories and for different levels. These challenges should be easily usable in a workshop format or in a competition.

This topic is suitable for 1 or 2 student(s) in the format of an on-site internship.

Required skills: we require someone with experience in programming and (at least) a basic knowledge on vulnerabilities and exploitation.

Optional: An extensive knowledge of vulnerability detection / exploitation in one or more categories is considered a plus (web applications, infrastructure, wireless networking, cryptography, steganography, reverse engineering, etc.).

Goals:

- Create multiple hacking challenges in multiple categories and for different levels.
- If the current framework has limitations, extend the framework.
- Work out workshops aimed at different audiences (e.g. first introduction to web application security, red/blue team training, etc.).
- Create challenges that only have 1 solution.
7. Threat intelligence framework

The goal of this internship is to facilitate a peering eye on the internet. When an attack is planned or has been executed, it’s usually possible to find traces (e.g. discussing the timing of a DDoS attack, sales of credit card numbers from a breach, bragging about defacing a popular website, etc.).

A basic search on a company name usually already yields millions of results. This information only includes results where the correct name is used, in a small set of languages, and where the search engine was permitted to crawl. Additionally, this information is just a ‘dumb dump’ of everything found related to a certain subject. We are looking for an internship student to create a threat intelligence framework to facilitate such searches (e.g. excluding everything found on the public website, including underground Russian forums known to post these things, etc.).

This topic is suitable for 1 student in the format of an on-site internship.

**Required skills:** we require someone with experience in programming.

**Optional:** knowledge on current threats or the financial sector is considered a plus.

**Goals:**

- Create a threat intelligence framework with automated search functionality.
- Implement multiple search sources.
- Create an indexing and scoring system for sources.
- Create model for information sharing based on existing standards (TLP, STIX, TAXII)
- Create an easy-to-use web interface.
- Document all created material.
- Create a presentation outlining the current threat landscape in the financial sector, the chosen approach for search sources and functionality, and open points.
8. Alignment of penetration testing methodologies with industry standards

The EY FSO security team has a long history of performing penetration tests to aid clients in the detection and remediation of vulnerabilities in their various components (including web applications, IT infrastructure, phone banking applications, etc.). On the other hand, the financial sector has seen the introduction and reinforcement of various laws and regulations requiring penetration tests to be performed aligned with various standards.

We have documented methodologies for various security assessments we perform, but need to verify if there are components that need to be further aligned / better specified. Further on, we could use a methodology that includes more hands-on information. Including this type of information offers a good introduction to the world of penetration testing.

This topic is suitable for 1 student in the format of an on-site internship.

**Required skills:** we require someone with good knowledge of web applications and IT infrastructure, and basic knowledge on security vulnerabilities / penetration testing.

**Optional:** hands-on experience with security testing is considered a plus.

**Goals:**

- Align our current methodologies to the various applicable standards.
- Further document these methodologies with hands-on information acquired through secure testing (in a demo-environment).
- Align the checklists used during security assessments to the applicable methodology.
9. Penetration testing approach for web application frameworks

A penetration test is somewhere between an art and a science: a methodology is strictly followed to ensure a consistent approach is applied during the preparation, testing and reporting phases. Because every test is different (and you never know in advance what you will encounter), the person executing the test makes the difference between ‘an automated test’ and a thorough security assessment.

Many websites are built using a wildly distributed framework. Much information about these frameworks is available on many different locations online, and can be very useful during a penetration test. We would like to have a complete database of most common frameworks (front-end and back-end) with all relevant information (e.g. default administrative credentials, vulnerabilities in specific versions, usage of phpmyadmin, etc.).

This topic is suitable for 1 student in the format of an on-site internship.

Required skills: we require someone with basic knowledge of web applications and the existing frameworks.

Optional: strong knowledge of different front-end and back-end frameworks or vulnerabilities in web application frameworks is considered a plus.

Goals:

- Create a database suitable for the information that will be collected.
- Create an easy-to-use overview for all of this information.
- Collect extensive information on the most common web application frameworks.
- Ensure the currently used checklists used for web application testing integrate the web application frameworks information.
- [Optional] Link the information collected with the existing ‘findings database’.
10. Penetration testing workshop

To give students a good idea of how a penetration test is performed, EY gives workshops at multiple colleges. Such a workshop provides the opportunity to students to get a (first) hands-on experience of executing a penetration test, while staying in a secure environment with the support from experienced ethical hackers.

Although every workshop can be customized, the same virtual testing environment can be used. This environment is set-up in such a way that students can go from the reconnaissance phase to the exploitation phase in a relative short amount of time, but provides more possibilities for enthusiasts that quickly reach the goal.

This topic is suitable for 1 student in the format of an on-site internship.

**Required skills:** we require someone with basic knowledge of security vulnerabilities, Windows and Linux.

**Optional:** experience in penetration testing and a strong knowledge of securing systems is considered a plus.

**Goals:**

- Create a virtual environment to be used during the workshop.
- Configure the virtual environment for the currently existing scenario.
- Configure the virtual environment to enable multiple distinguished scenarios.
- Create sufficient documentation for participants and moderators.
- Create a supporting slide deck.
- Ensure that only the selected scenarios are feasible, and that the selected scenarios work as expected.
11. SharePointify the planning sheet

Many different planning tools exist, and each tool has its own strengths and weaknesses. Historically, and because of the specific needs of the security team, a simple Excel sheet on a shared drive is the solution used at the moment. Although this still works fine, we’re looking to migrate the planning to SharePoint. Some of the most important characteristics of the planning are:

- Automatic notification to the involved people when their planning is updated.
- Differentiation between confirmed and unconfirmed projects.
- An overview that provides a full view of all people and all projects in a certain timeframe.
- Additional information regarding projects.
- If possible, automatic synchronization with the existing Excel sheet to ensure the planning can be checked both online and offline.

This topic is suitable for 1 student in the format of an on-site internship.

Required skills: we require someone with basic knowledge of SharePoint.

Optional: experience in SharePoint programming and integration of Microsoft Office documents is considered a plus.

Goals:

- Create a SharePoint application for the planning.
- Ensure changes to people’s planning are automatically communicated to these persons.
- Ensure changes made between a certain period can be extracted easily.
- Ensure the SharePoint site and the Excel sheet synchronize their content.
- [If possible] Enable synchronization with an internal application to automatically retrieve project information.
- [Optional] Automatic synchronization with people’s Outlook agenda (from SharePoint to Outlook).
12. Brand monitoring framework

Every organization tries to have a good online exposure, in order to attract new customers, manage existing customer services and to ensure customers can find the organization 24/7. Although online exposure can be critical for the (continued) success of an organization, it can also be the success factor for an attacker.

The amount of information that can be found online, and the extensive details that can be found on organizations, is immense. Organizations often don’t think about looking at this information, but are overwhelmed with information when they try to find out what is published.

Apart from the official sources (the information that companies publish, knowingly or unknowingly, on their own websites), a lot of information can also be found using external sources. Apart from the darknet, a lot of useful information is often available without any form of protection, due to the lack of knowledge from individuals involved. Think about DNS records, online password dumps, mobile app stores, source code repositories, etc.

The goal of the brand monitoring framework is focused on the (recurrent) collection of publicly available information, to ‘know what is out there’. When information is deemed unnecessary or provides a risk, appropriate actions can be taken to remove this information.

This topic is suitable for 1 student in the format of an on-site internship.

Required skills: we require someone with a good knowledge of programming.

Optional: experience in python, scapy and Elastic Search is considered a plus.

Goals:

- Create a brand monitoring framework with the following functionality:
  - Clear overview of information published;
  - Sorting of information per type / source;
  - Distinction between new, updated or duplicate information;
  - Management of domains to scan; and
  - Possibility to automatically and manually provide input.
- Set up monitoring services for multiple sources.
- Document the framework.
13. Malware testbed

When new software is created, it’s important to ensure the quality is as expected before starting to sell the product. When malware is created for usage during a stealth security assessment, every aspect needs to be thoroughly tested to ensure no mistakes are made. This includes thorough testing of the behavior, functionality, and antivirus evasion techniques.

One of the techniques to achieve this thorough evaluation is to use a malware testbed. Using this testbed, the behavior of the malware can be closely inspected and monitored in a controlled environment, consisting of a wide variety of systems. In the end, it should even be possible to mimic the target environment to have tests as close to the reality as possible.

To decrease the time required to go through all of the testing, and to ensure the testing does not become a burden, automation of the most common tasks is required. A short, not exhaustive overview of tasks can be found below to provide a first idea:

- Provisioning of virtual machines;
- Installation of a variety of software on virtual machines;
- Running of certain tests, creation of monitoring reports, etc.; and
- Decommissioning of virtual machines and centralization of the test results.

This topic is suitable for 1 or 2 students in the format of an on-site internship.

**Required skills:** we require someone with a good knowledge of programming and malware.

**Optional:** experience with REMnux, Docker and Cuckoo is considered a plus.

**Goals:**

- Automatic provisioning of virtual machines.
- Creation of suitable virtual images.
- Automatic installation of a variety of software on the virtual machines.
- Creation of certain test scripts and usage of existing tools for the analysis.
- Centralization and interpretation of the test results.
- Document the framework.
14. Internal and External marketing campaign

Most people understand the value of proper marketing, usually with regards to a specific product to everyone willing to see (or not able to evade it). The EY FSO security team also understands this value, and is looking at a way to create a marketing campaign, targeted internally and externally.

Many people know EY, and most of them will know EY as ‘one of the big4’, an accounting firm. Although there’s nothing wrong with this, there’s more to EY (and the security team) than this. In order to ensure that colleagues, potential recruits and clients know what we do, the security team is looking into launching an internal and external marketing campaign. An intern would play a big role in this story, creating a marketing plan and starting the implementation (think about social media, press coverage, videos, etc.).

This topic is suitable for **1 student** in the format of an **on-site internship**.

**Required skills**: we require someone with a relevant background (marketing, communication, etc.) and an interest in technology.

**Optional**: experience in setting up / maximizing the benefit of social media account is considered a plus.

**Goals:**

- Create a marketing plan for both internal and external marketing.
- Set up relevant social media accounts, aligned with a specific strategy on usage and content.
- Creation of press material and a contact list.
- Creation of (animated) videos.
- Other implementations from the marketing plan.
15. Study on the merits, the security impact and the rollout of Data Loss Prevention

Over the past few years, a number of major organizational IT trends have been taking place in the financial sector. Sensitive personal and business data are typically (re)used and outsourced across different processes and handled by employees with various roles and clearances. This increases the likelihood of illegitimate disclosure. Additionally, the growing use of mobile devices is making it hard to secure a blurring corporate perimeter. Third, the regulatory landscape is changing, making liabilities more substantial than ever. Lastly, the centralized consolidation of large amounts of information for analytics and Big Data, exacerbates the severity of potential leaks manifold.

This topic is suitable for 1 student in the format of an on-site internship or a written thesis.

Required skills: we require someone with a relevant background.

Optional: experience in DLP is considered a plus.

Goals:

- Define and delineate Data Loss Prevention (DLP) and how it relates to / complements conventional security controls like awareness and access control.
- Define how different organizational areas (People, Process, Technology) are impacted by the rollout of a DLP program. A common misconception, for instance, is seeing DLP as a merely technological solution.
- Determine the most effective approach for putting in place DLP. Which changes are required before proceeding? Is there a feature set that is best prioritized for a first phase rollout, adding to the success of next stages?
- Elaborate on how a DLP program can help address the evolutions and concerns from the previous paragraph.