EY

Information Security

BeNe Internship topics 2016-2017

The better the question. The better the answer.
The better the world works

Building a better working world

The better the question. The better the answer.
The better the world works

What is EY's Information Security service line?

Organizations must be prepared to combat against, manage and mitigate cyber-attacks that can occur anytime, anywhere.

Nowadays, Information Technology provides the opportunity to get closer to customers and respond to them rapidly, which can significantly enhance the effectiveness and efficiency of a company's operations. Online technology enablers such as social media, mobile internet, cloud and 'smart' eCommerce and continually shaping our daily lives.

But at the same time, as organizations leverage new technologies, new risks emerge, and information becomes a viable threat. Therefore, companies thrive to put information security, data privacy and protection from IT threats at the forefront of their agenda.

Within EY Advisory, our BeNe Information Security service line has now more than 20 years of experience in improving the information and cyber security posture of industry leaders all over the globe. We are committed to help our clients achieve their business strategies by providing them with objective and independent assessments and advices.

Our global network of Advanced Security Centers (ASC's) sharing a cloud-based infrastructure is unique amongst our direct competitors, and we are the only firm within the "Big Four" to have a globally consistent set of solutions, methodologies and trainings.

What services do we offer to our clients?

Our interns are supervised by a talented and experienced team of security professionals that are involved in a wide variety of technical and non-technical projects.

Technical Projects:

- Web application ethical hacking
- Infrastructure ethical hacking
- Source Code Reviews
- (D)DOS, Load and Stress Testing
- PKI Assessments
- Forensic Investigations
- Advanced Malware Protection
- Network Infrastructure
- Security Operation Centers
- Threat Intelligence

Non-Technical Projects:

- Security Awareness
- Information Security Risk Analysis
- Security program Development
- Physical Security Assessments
- Data Privacy
- Security Maturity Assessments
- Business Continuity
- Disaster Recovery
- Security Dashboards
- Security Program Transformations

What profiles are we looking for?

We are looking for talented and dynamic students currently finalizing their education, and having a strong interest in the field of Cyber Security and Data Privacy.

You are pursuing studies in IT, (Applied) Computer Sciences, Engineering, Law or a related field of expertise, and you are interested in IT risk, Information Security or Data Privacy.

We appreciate young professionals that are result-oriented, and that can demonstrate strong analytical, reporting and presentation skills. Proactivity and the ability to work both independently and within a team are strong assets.

We furthermore require a good oral and written knowledge of English.

How can we contribute to launch your career?

As an intern within our Information Security service line, you are part of our high performing team. Your personal and professional growth is at the heart of our culture, and you will get the freedom to take your first steps towards a successful career path.

The remainder of this document describes the internship topics that we currently propose for the academic year 2016 – 2017.

You can apply now by contacting our Internship Coordinators. When doing so, please let us know where you are currently studying, when the internship should/could take place, as well as which topic(s) you are the most interested in.

Do you want to suggest your own topic?

The topics listed in this document are only suggestions, and we are open to discuss any other research topic that is not listed and that you might want to propose, as long as you can demonstrate an added value for EY's Cyber Security & Data Privacy service line.

Arvid Vermote
Manager
arvid.vermote@be.ey.com
0472/67.00.30

François Santy
Senior
francois.santy@be.ey.com
0478/53.90.43

Internship topics

1. Building a proof-of-concept application profiling and anomaly detection engine

A. Objective

To develop an application profiling engine that can detect anomalies based on derivation of standard user behavior.

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- Develop a web application profiler that is capable of, through the analysis of application usage, compose a profile as what can be considered as standard application behaviour.
- Build an anomaly detection engine that identifies derivations from the previously composed normal usage "profile".
- Identify and implement additional intelligence and analysis techniques to further strengthen the anomaly detection engine

C. Outcome

- A report documenting the internship, i.e. research and implementation of the expected deliverable, including a description of the project plan and the approach
- Profiler & anomaly detection engine
- A presentation to the information security team

2. Development of an IoT risk assessment methodology

A. Objective

IoT (Internet of Things) combines connectivity with sensors, devices and people, enabling a form of free-flowing conversation between man and machine, software and hardware. With the advances in artificial intelligence and machine learning, these conversations can enable devices to anticipate, react, respond and enhance the physical world in much the same way that the internet currently uses networks and computer screens to enhance the information world.

While the IoT is entering daily life more and more, security risks pertaining to IoT are growing and are changing rapidly. In today's world of "always on" technology and not enough security awareness on the part of users, cyber attacks are no longer a matter of "if" but "when."

In this context, EY is looking to develop a security assessment methodology that will encompass all aspects of IoT technology: devices, operating systems, applications, etc.

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- Provide a state-of-the-art research on current IoT technologies in use, and derive a taxonomy of these technologies (typical operating systems,...).
- Design an assessment methodology that will provide ethical hackers a framework of reference to assess the risks related to the use of IoT technologies within organizations.

C. Key references

- http://www.scmagazineuk.com/cyber-security-of-the-fridge-assessing-the-internet-of-things-threat/article/495675/
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

3. Development of Privacy Compliance Metrics

A. Objective

In order to make Europe fit for the digital age and facilitate business by simplifying rules for companies across the region in line with the European Single Market Strategy, the European Commission has put forward a EU Data Protection Reform in January 2012. Three years later, the European Parliament, the Council and the Commission reached an agreement on a General Data Protection Regulation (GDPR) defining data protection standards and laws across the EU. Approved in April 2016, the regulation is expected to come into force on the 25 May 2018, giving company across the region two years to ensure they become compliant when these new rules.

Addressing the compliance, budgetary and risk factors associated with the introduction of the Regulation will prove challenging for many organization, especially because they are all concerned, whatever their size or revenue. Organizations that fail at complying with the regulation furthermore take the risk of being fined up 20 000 000€ or up to 4% of the total worldwide turnover of the preceding financial year, whichever is higher).

In this context, the goal of the project is to identify how a company can periodically control and measure its adherence to the Regulation requirements through the use of metrics (measurable outputs of work). These metrics shall be useful to company boards to enhance organizational governance and support management in making privacy-related decisions

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- To define of set of smart (specific, manageable, actionable, relevant and timely) metrics specifics to privacy: identify which activities are necessary to achieve compliance to the GDPR and identify metrics that measure those activities.
- To create guidance with regard to metrics implementation and interpretation.

C. Key references

- http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1471849088455&uri=CELEX:32016R0679

4. Development of a Privacy Impact Assessment Tool

A. Objective

In order to make Europe fit for the digital age and facilitate business by simplifying rules for companies across the region in line with the European Single Market Strategy, the European Commission has put forward a EU Data Protection Reform in January 2012. Three years later, the European Parliament, the Council and the Commission reached an agreement on a General Data Protection Regulation (GDPR) defining data protection standards and laws across the EU. Approved in April 2016, the regulation is expected to come into force on the 25 May 2018, giving company across the region two years to ensure they become compliant when these new rules.

Addressing the compliance, budgetary and risk factors associated with the introduction of the Regulation will prove challenging for many organization, especially because they are all concerned, whatever their size or revenue. Organizations that fail at complying with the regulation furthermore take the risk of being fined up 20 000 000€ or up to 4% of the total worldwide turnover of the preceding financial year, whichever is higher).

In this context, the goal of the project is to is to develop a tool (Privacy Impact Assessment) allowing a company to identify its gaps to leverage and extend its current data protection capabilities by following a structured and well-defined roadmap that is aimed at ensuring compliance with the EU regulation. The tool shall enable enough flexibility to be tailored to companies of different sizes, working in different industry sectors, both nationally and internationally, and should consider integration with additional regulations.

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- To Analyze the regulation requirements regarding data processing identification, registration and risk assessment;
- To develop a tool to perform and register Privacy Impact Assessments (the tool shall be able to identify common issues with the regulation requirements).

C. Key references

- http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1471849088455&uri=CELEX:32016R0679

5. Creating a data analysis flow and model for threat intelligence

D. Objective

To create a data model for the normalization and analysis of threat information and an API to allow clients to consult this information and compare it with their internal data/assets.

E. Aspects that should be covered

- Identification of (open) sources that feed threat intelligence information
- Identification of corporate data sources required as base data for analysis
- Creation of sample data as basis for analysis
- Creation of normalization schemes, parsers and data model
- Development of REST API through which the threat information can be downloaded in multiple formats

F. Outcome

- An report documenting the internship, i.e. research and implementation of the expected deliverables, including a description of the project plan and the approach
- Data model documentation
- REST API
- A presentation to the information security team

6. Benchmarking a file analysis framework against online scan engine

A. Objective

Nowadays, companies of all sizes are subject to the risk of malware infection and, as such, have a need for integration of incident response in their activity towards cyber security. When there are few to no resources available on a permanent basis, the activity can be kept to its strict minimum which would be performing files analysis. The goal would be, when receiving a suspicious file, to determine whether it is a menace.

Such a task can sometimes be summed up in one sentence: "send the file to VirusTotal and wait for the result". Nevertheless, what if the organization does not want files to be sent over the Internet to be analyzed? Can the file analysis still be performed, locally, without requiring extensive manual actions and with similar – if not better – results ?

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- Determine the risks and advantages of the usage of each tool
- Know the limits of the framework, determine what are the "blind spots" left when using it
- Think of possible complementary tool(s)

C. Key references

- http://irma.quarkslab.com/
- https://irma.readthedocs.io/en/latest/
- https://www.sstic.org/media/SSTIC2015/SSTIC-actes/irma_incident_response_and_malware_analysis/SSTIC2015-Article-irma_incident_response_and_malware_analysis-quint_lone-sang_dedrie.pdf

7. Evaluation of breach detection/protection solutions

A. Objective

To perform a market study and comparison of different incident breach detection/protection solutions and common characteristics

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- Definition of incident breach detection/protection
- Overview of vendor and product landscape
- Definition of functional requirements
- Analysis of license models
- Definition of evaluation criteria, including expected IOC (indicators of compromise)

C. Outcome

- A report documenting the internship, i.e. research and implementation of the expected deliverable, including a description of the project plan and the approach
- Evaluation methodology for incident breach detection/protection solutions
- Results of the evaluation
- Description of opportunities for enhancing an organization's security operations and incident response
- A presentation to the information security team

8. Development of a convergence model based on recurrent compliance security control frameworks

A. Objective

With today's companies being subject to multiple compliance requirements, it can be a daunting and challenging task to track and ensure conformity with many different requirements arising from multiple regulation sources.

This suggests the development of an integrated way of working resulting in only one time implementation and testing of combined controls, therefore saving time and resources in control implementation.

The purpose of the internship therefore consists in the consolidation of the controls coming from different security control frameworks and converge them into one comprehensive set of general controls.

B. Aspects that should be covered

The intern is expected to cover the following aspects:

- Conduct a state-of-the art analysis of existing security control frameworks
- Identify areas where different security control frameworks prescribe a similar approach, and converge these into a consolidated general control
- Develop an Excel tool to structure the consolidated general control list and associated individual framework controls logically
- Extend the Excel tool in an assessment questionnaire with the purpose of being able to determine the level of compliance of a company with the considered compliance requirements based on the consolidated general control list.

C. Outcome

- A report documenting the internship, i.e. research and implementation of the expected deliverable, including a description of the project plan and the approach
- An excel tool with the consolidated controls
- A presentation of the results to the security team

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ey.com