EY Cybersecurity Internships 2017 - 2018

Information for internships & theses

Building a better working world

Cyber Security in EY

Organizations must be prepared to combat against, manage and mitigate cyberattacks 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 are continually shaping our daily lives. But at the same time, as organizations leverage new technologies, new risks emerge, and information is under constant threat from attackers.

Therefore, companies thrive to put **information security, data privacy and protection** at the forefront of their agenda. EY Advisory 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.

Services we offer to our clients

- Advanced Malware Protection
- Business Continuity Management
- (D)DOS, Load and Stress Testing
- Disaster Recovery
- Forensic Investigations
- Information Security Risk Management
- IT Audit
- Infrastructure Ethical Hacking
- Network Infrastructure
- Physical Security Assessments
- Privacy and Data Protection
- Awareness Campaigns
- Maturity Assessments
- Security Operation Centers
- Program Transformations
- Source Code Reviews
- Threat Intelligence
- Web application ethical hacking

Why should you choose EY

"The best thing about my internship was that I got the freedom to explore every option I thought was interesting. This freedom contributed to an internship that was never dull nor boring, but also pushed me to learn a lot about a subject I did not have much experience with."

Geoffrey Van Den Berghe, intern 2016

The EY Cybersecurity Team has been offering internships to Belgian and international students since 2006. During the past decade we learned that students are more than just potential interns, they are educated and skilled individuals.

We look for the mindset

- Students with the mindset to achieve and persevere can easily catch our attention with out of the box ideas, especially in the field of Cybersecurity. Therefore we encourage everyone to apply for an internship who believe they have what it takes. After an initial interview to determine our mutual interests, we assign a subject matter expert who functions as your primary contact.

We contribute to launch your career

- As an intern, 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**. We can offer interns 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. 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).

"A few days after starting my internship, my mentor told me that I'll be using a brand new tool called "Apache NiFi", which was completely different from the initial idea, so it was quite a funny start."

Dardan Prebeza, intern 2016

- The remainder of this document describes the internship topics that we currently propose for the academic year 2017-2018. 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.

Contact us at : internships.infosecurity@be.ey.com

Overview internship topics

Subjects for bachelor students

- Benchmarking a file analysis framework against online scan engine
- Creating a data analysis flow and model for threat intelligence
- Development of an IoT risk assessment methodology
- Development of a Privacy Impact Assessment Tool
- Develop a convergence model based on recurrent compliance security control frameworks
- Evaluation of breach detection/protection solutions
- Internal and External marketing campaign
- Implement an automatic reporting tool

Subjects for master students

- Exploring ransomware
- Legacy systems security testing
- Cyber security aspects of space trade
- Machine learning in the SOC
- Cyber warriors and cyber criminals
- Develop a secure coding standard
- Enforcing and controlling secure development within the organizations
- Secure coding standards
- Information Asset Management
- Role-based access - information model
- Identity & Access Management (IAM) Managed Service Offering

The following list of example topics **is not an exhaustive list**, we can easily update these topics to fit your needs or interests and any topic you propose that is within our line of expertise will be taken into account. In other words, **if you have an out of the box idea we can help.**

Benchmarking a file analysis framework against online scan engine

Objective & context

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 ?

- 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

Aspects that should be covered

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

Creating a data analysis flow and model for threat intelligence

Objective & context

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.

Expected outcomes

- 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

Aspects that should be covered

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

Development of an IoT risk assessment methodology

Objective & context

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.

Aspects that should be covered

1. Provide a state-of-the-art research on current IoT technologies in use, and derive a taxonomy of these technologies (typical operating systems,...).

2. 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.

Creating a data analysis flow and model for threat intelligence

Objective & context

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.

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

Aspects that should be covered

1. Analysis of the the regulation requirements regarding data processing identification, registration and risk assessment;
2. Development of a tool in order to perform and register Privacy Impact Assessments (the tool shall be able to identify common issues with the regulation requirements).

Development of a convergence model based on recurrent compliance security control framework

Objective & context

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.

Expected 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

Aspects that should be covered

1. Conduct a state-of-the art analysis of existing security control frameworks
2. Identify areas where different security control frameworks prescribe a similar approach, and converge these into a consolidated general control
3. Develop an Excel tool to structure the consolidated general control list and associated individual framework controls logically
4. 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.

Evaluation of breach detection protection solutions

Objective & context

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

Expected 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

Aspects that should be covered

1. Definition of incident breach detection/protection
2. Overview of vendor and product landscape
3. Definition of functional requirements
4. Analysis of license models
5. Definition of evaluation criteria, including expected IOC (indicators of compromise)

Internal and External Marketing Campaign

Objective & context

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.).

Profile

The background of the student is independent to the subject as we are looking for someone who has the mindset to work on this challenge, is an open communicator and has experience with running a digital brand across a campaign.

Aspects that should be covered

1. Create a marketing plan for both internal and external marketing
2. Set up relevant social media accounts, aligned with a specific strategy on usage and content
3. Creation of press material and a contact list
4. Creation of (animated) videos
5. Other implementations from the marketing plan

Implementation of an automatic reporting tool

Objective & context

One of the most crucial, but also most time consuming tasks during any security assessment (such as a penetration test or red team test) is creating the report. This report is often the only end-result of such an assessment and is presented to management and above. Because such a report details all findings that came up during the assessment and because every environment (and thus findings) is different, a lot of effort goes into each report.

Expected outcome

A wide variety of automatic reporting tools that could assist in creating a report exist, but we have no clear overview of the benefits and downsides of these tools. After a market analysis and selection of the best candidate we expect a complete implementation of a reporting aid that is capable of handling multiple report templates and is aligned with the SharePoint findings database.

Aspects that should be covered

1. Research the possible tools and create an overview of benefits and downsides
2. Aid in the selection of a candidate
3. Create an installer / installation with sufficient documentation
4. Ensure all current templates are integrated and can be selected, updated and used
5. Implement a link with the SharePoint findings database
6. Create sufficient documentation for the security team

Exploring ransomware

Objective & context

The growing threat of ransomware is reaching unforeseen levels (clearly demonstrated during the global WannaCry outbreak), and the most concerning factor herein is the simplicity. While the concept is clear, the internal technical aspects of ransomware strains are different. In many cases vulnerabilities in the inner aspects arise rendering the malware ineffective (or at least less critical). For many variations tools exist to decrypt your data for free.

A lot of research has been carried out already (by technology companies, by governments, by independent researchers) but it is hard to consolidate all this information. What we are interested in are the origins (how many strains are known, how many authors are there), the usage (single action or ransomware as a service), how many were properly implemented and for how many are decryption tools available due to guilt, etc.

Aspects that should be covered

1. We are mostly looking at a theoretical approach but would be more than happy to include a very hands-on approach if the students has good experience in reverse engineering and cryptography

2. From a more theoretical point of view, we are very interested in know the who, how, what and why. Perhaps some interesting trends can be deduced (e.g. trends in attack vectors, vulnerabilities in strains, etc.) that can be used in the next big outbreak

Legacy systems security testing

Objective & context

IT tends to focus on new systems and technologies, while IT Operations teams within FSO companies heavily rely on legacy systems. These systems often represent a large part of the code base of business critical applications; legacy systems therefor often represent a single point of failure.

New systems are usually subject to periodic patch cycles and applications receive security updates,
increasing the risk related with unauthorized access to customer data. Because legacy systems weren't always developed with security in mind, customer data can often more easily be access through these legacy systems (such as mainframes, old middleware, etc.).

To paint the picture a little better, imagine a network where customer data is ultimately managed by legacy systems using software written 40 years ago, whereby systems are running operating systems years past its end-of-life, who exchange data in clear text and leverage services that have more holes than Swiss cheese, and which should be accessible using internet APIs. Even though this legacy setup has been working rock solid for years, new attacks can change this paradigm. In the last years, the penetration testing community has been catching up with this issue through several new tools, techniques and methodologies. All of this has been possible without being forced to learn old programming languages or becoming experts in a mainframe architecture.

Aspects that should be covered

1. Research the most common implementation of legacy systems security testing
2. Thoroughly evaluate these procedures and identify incorrect procedures
3. Connect the methodology to risks identified in day-to-day activities
4. Create sufficient documentation for immediate use

Cyber Security aspects of space trade

Objective & context

Space trade and space economics are still a bit of science fiction topics, but these days more and more serious scientific publications appear on how trade in space should be governed and executed. Serious scientists have written about risks and potential regulations, and practical problems to overcome. These recent events shift from the conceptual thinking to a practical implementation.

We are looking for a student with an economics background to look into the considerations of space trade from a cyber security perspective. The expected outcome is a master thesis that does not aim at providing _the_ definite answer to this question but takes current information (on space trade and (potentially) applicable cyber security aspects) to define a thorough analysis.

We are looking for a student who...

- Is about to get a master degree in economics or in computer science with demonstrable affinity in the other.
- Has an open mind and can take a creative go at this question.
- Has an advanced knowledge of English.

Aspects that should be covered

1. The end result should at least be a thorough, balanced but complete article that can be published within EY Global or by EY to the wide public

Machine learning in the SOC

What can and cannot be learned and predicted?

Objective & context

In the Security Operations Center trained operators are looking for 'the unexpected' to identify incidents (such as a DDoS attack, malware outbreak, etc.) and to act swiftly to remediate. Machine learning in the SOC is already being implemented and has the ability to detect anomalous behavior. This technique is not new, but there is still a far way to go for the computer to beat human experience and 'gut feeling'.

Currently human operators are already aided by software (rule-based mostly), but we want to research what it would take to fully remove human interference from this process. This will include a good understanding of the current approach, the strengths and possibilities and machine learning but also a good understanding of its shortcomings. In the end, the main question to answer is what can and cannot be learned and predicted in such an environment.

We are looking for a student who...

- Is about to get a master degree in computer science/AI
- Advanced knowledge of machine learning
- At least basic knowledge of the functioning of a SOC

Cyber warriors and cyber criminals ethics in cyber warfare

Objective & context

The difference between cyber criminality and cyber warfare is often denoted as the real-world physical impact; whereby cyber criminality will often have a clear impact to the real world, cyber warfare adds the physical impact to such activities (cyber warfare results in people being physically harmed in the real world). The image of the hacker wearing a hoody at night in a basement is long gone; organized crime and even state actors have found their way to cyberspace. The threat of real-world physical damage was probably first widely demonstrated by Stuxnet, and the threat of cyber criminals (or warriors) taking over traffic lights, nuclear power plants and water filtration plants is more prominent than ever.

What is still unclear at this point is who exactly these cyber warriors are and if they stick to the same ethics as during 'real war' (think of the international criminal court where people can be trailed for war crimes). We want to study the motives of cyber criminals/warriors, if they perceive cyber warfare different than war and how such people are pushed to the point of no return.

We are looking for a student who...

- Is about to get a master degree in criminology, law, psychology or sociology.
- Has awareness involving the world of cybercriminals.

Aspects that should be covered

1. Research the available information on the topic; specific will be drawn up depending on the background of the student

Enforcing and controlling secure development within organizations

Objective & context

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.

Aspects that should be covered

1. Extensive understanding of principles of secure development
2. 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
3. Describe the advantages of secure development being enforced within organizations
4. Describe possible disadvantages (especially on the business side) of enforcing secure development principles
5. 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

Secure coding standards

Their reason for existence and current gaps

Objective & context

Programming is something many people learn at school, on the job or in their free time. Because many people learn this in different ways, there are a lot of programming styles that are used. Something that is often not part of learning to program is secure coding (i.e. writing code with a focus on preventing vulnerabilities and performing reviews to identify any vulnerabilities that have been introduced). Secure coding standards can be created for each programming language, platform or framework in which security vulnerabilities can be introduced as a result of programming.

Of course secure coding standards have to be up to date with the current trends. We would like to have a clear overview of programming languages, platforms and frameworks for which secure coding standards are present and what their current status is (i.e. are they up-to-date to current threats, are they well maintained, are they exhaustive, do they have a large user-base, etc.). Other than the research aspect we want to develop a generic secure coding standard (that is applicable to all, or a subset of, programming languages and covers most recurrent aspects) and expand the current secure coding standards base with some missing standards for emerging languages and frameworks.

Aspects that should be covered

1. Research the current status of needs (where would secure coding standards be needed) and actual status (currently available standards)
2. Create a generic standard that could be used for any programming language and covers the most prominent / recurring secure coding errors
3. Contribute to the community by creating or expanding secure coding standards for emerging languages and frameworks

Information Asset Management

Objective & context

Companies manage information assets on different levels: from data to applications and business processes. Goal of the internship is to perform research on which levels of information assets need to be controlled / managed by a financial services organization, who should have ownership and what tooling exists to manage each type of information asset.

The topic is heavily research-based. We expect the student to analyze existing best-practice frameworks to come to a conclusion on how these could be applied in practice. This topic is suitable for 1 student in the form of an on-site summer internship There is a possibility to combine this subject with the 'Role-based access - information model' subject and to link both subjects. In this case, it could be a combined effort of two students.

Aspects that should be covered

1. Benchmark different best practice frameworks
2. Summarize and conclude which information asset management model would best suit a financial services company
3. Describe roles & responsibilities for each information asset layer
4. Research existing tooling and conclude which types of tools exist to manage information assets.

Role-based access
Information model

Objective & context

Best practice model, ownership & tooling

One of Identity & Access Management's main concepts is Role-Based Access Control (RBAC). It allows an organization to efficiently distribute accesses based on a person's job function, rather than his individual needs. For large organizations, this often means a large productivity gain, allowing easier attribution of access rights.

Within a role-based access model, there are different layers of access that tie into each other. In effect, access is usually defined on different levels: organizational, departmental, functional, regional,... Goal of this project will be to define which levels are used in a best-practice model, and to describe how they tie in together.

If possible, the link is made to the subject about Information Asset Management, making the link between the different information asset components, and the way access is defined.

Aspects that should be covered

1. Describe the concept of role-based access
2. Outline which layers can be built into an RBAC model
3. Describe the advantages and disadvantages of every layer
4. Create a fictive scenario of a financial services company and describe which setup would be best

Identity & Access Management

Managed Service Offering

Objective & context

Financial services companies are looking to outsources more and more of their operations to third parties. This is what they call 'managed services'. The goal of this internship is to research and describe if the same concept can be used for Identity & Access Management services. Which services are offered or wanted on the market, and to which extent are they interesting for EY to offer.

Aspects that should be covered

1. Describe the concept of 'managed services'
2. Describe how the concept could be applied to the Identity & Access Management domain
3. Create an overview of IAM managed services that exist in the market
4. Define managed services that do not exist yet, but that could potentially be interesting
5. Assess which services are interesting for a consulting firm, such as EY

Solve the riddle

083 111 108 118 101 032 116 104 101 032 114 105 100 100 108 101 032 097 110 100 032
112 114 105 110 116 032 111 117 116 032 116 104 101 032 114 101 115 117 108 116 032
116 111 032 114 101 099 101 105 118 101 032 097 032 103 105 102 116 046 013 010

PD94bWwgdmVyc2Ivbj0iMS4wIiBlbmNvZGluZz0iaXNvLTg4NTktMSI/PjxzdmcgdmVyc2Ivbj0iMS4xIiBp
ZD0iQ2FwYV8xIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHhtbG5zOnhsaW5rPSJo
dHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rIiB4PSIwcHgiIHk9IjBweCINCgkgdmlld0JveD0iMCAwIDU
3IDU3IiBzdHlsZT0iZW5hYmxlLWJhY2tncm91bmQ6bmV3IDAgMCA1NyA1NzsiIHhtbDpzcGFjZT0icHJlc
2VydmUiPg0KPHBhdGggZD0iTU3LDEyLjAwMkg0MS43NDFDNDIuNTU2LDEwLjgzNyw0Myw5LjQ1My
w0Myw3Ljk5NWMwLTEuODc1LTAuNzI2LTMuNjMzLTIuMDQzLTQuOTVjLTIuNzI5LTIuNzI5LTcuMTctMi
43MjktOS44OTksMA0KCWwtMi44MjksMi44MjlsLTIuODI4LTIuODI5Yy0yLjcyOS0yLjcyOS03LjE3LTIuNz
I5LTkuODk5LDBjLTEuMzE3LDEuMzE3LTIuMDQzLDMuMDc1LTIuMDQzLDQuOTVjMCwxLjQ1OCwwLjQ0
NCwyLjg0MiwxLjI1OSw0LjAwNw0KCUgwdjE0aDV2MzBoNDh2LTMwaDRWMTIuMDAyeiBNMzIuNDcyLD
QuNDU5YzEuOTUtMS45LjNS4xMjItMS45LjNy4wNzEsMEM0MC40ODIsNS4zOTksNDEsNi42NTQ
sNDEsNy45OTUNCgljMCwxLjM0LTAuNTE4LDIuNTk2LTEuNDU3LDMuNTM1bC0wLjQ3MiwwLjQ3Mkgy
NC45MjlsNC43MTQtNC43MTRsMCwwTDMyLjQ3Miw0LjQ1OXogTTE2LjkxNiwxMS41MS0wLjQ3MkMzMC
MzktMC45MzktMS40NTctMi4xOTUtMS40NTctMy41MzVjMC0xLjM0MSwwLjUxOC0yLjU5NiwxLjQ1Ny0
zLjUzNmMxLjk1LTEuOTQ5LDUuMTIyLTEuOTQ5LDcuMDcxLDBsMi44MjgsMi44MjlsLTMuNTM1LDMuNT
M1DQoJYy0wLjIwNywwLjIwNy0wLjM5NywwLjQ0MS0wLjU4MSwwLjY4OWMtMC4wNTQsMC4wNzMtMC
C4xMDcsMC4xNTItMC4xNTksMC4yMjljLTAuMDYsMC4wODgtMC4xMjMsMC4xNjctMC4xOCwwLjI2aC00
Ljk3Mg0KCUwxNi45MTYsMTEuNTE6IE0yLDI0LjAwMnYtMTBoMTQuNTU5aDQuNzMzaDIuMjU1SDI4djE
wSDVIMnogTTI4LDI2LjAwMnYtMkg3di0xMkgyOHogTTcsNDAuMDAyaDIxdjE0SDdWNDAuMDAyeiBNMz
AsNTQuMDAydi0xNGgyMQ0KCXYxNEgzMHogTTUxLDM4LjAwMkgzMHYtMTJoMjFWMzguMDAyeiBNNT
UsMjQuMDAyaC0ySDMwdi0xMGg5Ljg5OUg1NVYyNC4wMDJ6Ii8+PGc+PC9nPjxnPjwvZz48Zz48L2c+
PGc+PC9nPjxnPjwvZz48Zz48L2c+PGc+PC9nPjxnPjwvZz48Zz48L2c+PGc+PC9nPjxnPjwvZz48Zz48L
2c+PGc+PC9nPjxnPjwvZz48Zz48L2c+PC9zdmc+DQo=

01000111 01101111 01101111 01100100 00100000 01101100 01110101 01100011
01101011 00100001

Contact us at: internships.infosecurity@be.ey.com

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/or 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/be