EY FSO Cyber Security

Internships 2024-2025

Building a better working world

Phishing and social engineering methodologies for the future

Context

Phishing attacks are getting more and more difficult with always improving security mechanisms that can analyze and identify malicious intent in emails. As attackers keep evolving their techniques, we, as security professionals, should adopt these techniques to showcase the dangers to our clients. The goal of this internship is to investigate how the current and future security products work, and how these can be bypassed. It's also key to investigate other social engineering techniques like Vishing, Smishing, etc.

Internship objectives

1. Investigate and analyze the history of Phishing and Social Engineering techniques
2. Understand the different security mechanisms that prevent these types of attacks (Secure Email Gateway, SPAM filters, Web proxies, etc.)
3. Develop techniques that bypass the different blocking products and make Phishing successful.
4. Develop different Phishing scenario's (Malicious Link/Attachment) which can easily be used as templates for real Phishing Campaigns
5. Develop other Social Engineering capabilities, like spoofing telephoner numbers, etc.

Internship requirements

- Technical background, allowing to understand low-level concepts, protocols and techniques
- Curiosity around Hacking and the Offensive Security mindset
- out-of-the-box thinking

Values

- Strong communication skills in English
- Eagerness to learn
- Determination

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Developing a stealthy Mythic Agent

Context

Join us in developing a stealthy Mythic Command and Control (C2) agent using C. This project addresses the growing sophistication of cyber threats, aiming to create an undetectable C2 agent that ensures secure and reliable command channels. Interns will gain valuable experience in advanced cybersecurity techniques, contributing to tools that protect critical information systems against advanced persistent threats.

Internship objectives

1. Get to know the Mythic C2
2. Investigate the current challenges C2 payloads face
3. Develop a custom Mythic C2 agent
4. Use techniques that bypass the different blocking products and make the agent stealthy
5. Create documentation regarding the findings

Internship requirements

- Technical background, allowing to understand low-level concepts, protocols and techniques
- Curiosity around Hacking and the Offensive Security mindset
- out-of-the-box thinking

Values

- Strong communication skills in English
- Eagerness to learn
- Determination

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Incident Response Playbooks

Context

Being adequately prepared to deal with cyber attacks is crucial for any company. Incident Response (IR) Playbooks play a critical part in that readiness, as it allows for a swift and structured response effort to specific incidents. Research what makes a good IR Playbook, then create one or more. Optionally create an exercise to test the playbook and enhance it. Research good metrics to measure the effectiveness of IR Playbooks.

Internship objectives

1. Research state of the art incident response processes and procedures
2. Create one or more Incident Response Playbook for specific attack scenarios
3. (Optional) Create a table-top scenario to test the created playbook(s)
4. Research how to effectively measure the success of IR Playbooks

Internship requirements

- Understanding of security incidents
- Strong English skills
- General cyber security knowledge

Values

- Autonomy
- Critical thinking

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Security Events Simulation

Context

Any company should have processes to effectively react to cyber incidents. Testing these processes to ensure they are adequate without impacting the company can be challenging. Research tools that can generate security events in the logs, evaluate them in a test environment and determine the best option. Simulate scenarios with the chosen tool and test them to validate their effectiveness.

Internship objectives

1. Research and document the different tools that offer the desired functionality
2. Create and environment to test the different tools
3. Test the tools and document the results
4. Create simulated scenarios with the chosen tool
5. Test the created scenarios

Internship requirements

- Understanding of security incidents
- Strong English skills
- General cyber security knowledge

Values

- Autonomy
- Critical thinking

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

FiDA's Role in Enhancing Trust and Security in CIAM

Context

The European Union's Financial Data Access (FiDA) framework is an initiative that aims to increase trust and security within Customer Identity and Access Management (CIAM) systems by early 2027. Recognizing the implications FiDA will have, we are committed to proactively navigating these changes by ensuring our clients are equipped with the necessary insights to seamlessly transition to the new framework, maintaining compliance while delivering secure and dependable services. Your role will be crucial in clarifying the current operational practices, pinpointing the necessary changes, and detecting the appropriate tools to ensure a successful and smooth implementation.

Internship objectives

1. Initiate an In-Depth Study of FiDA: Begin by thoroughly researching the FiDA framework to gain a comprehensive understanding of its objectives, requirements, and the potential impact on CIAM systems.
2. Conduct a Gap Analysis: Review current CIAM systems and practices against FiDA requirements to pinpoint discrepancies and areas requiring improvement.
3. Develop a Compliance Roadmap: Formulate a strategic plan that details the necessary steps for our clients to comply with FiDA regulation.
4. Develop Training Programs: Design a training curriculum that addresses the new FiDA regulations, their operational implications, and compliance best practices for staff and clients.
5. Identify and Propose a Value-Adding Initiative: As an intern, take the initiative to uncover a unique opportunity or challenge within the FiDA transition process.

Internship requirements

- Foundational understanding of CIAM concepts
- Ability to seek out, evaluate, and integrate industry best practices and standards into the methodology

Values

- Analytical Skills
- Positive Mindset
- Strong Communication and Writing Skills in English

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

IAM and Capture the Flag (CTF)

Context

CTF competitions are games that challenge and train cybersecurity professionals using real-world scenarios. Since Identity and Access Management (IAM) is crucial for protecting digital identities, creating an IAM-focused CTF platform can help to discover different IAM obstacles. This platform will allow participants to tackle various IAM challenges, improving their understanding and encouraging innovative solutions in this area. The goal is to have a ready product which can be used by our clients.

Internship objectives

1. Study and understand IAM concepts and common vulnerabilities.
2. Develop realistic IAM challenges that mimic real-world vulnerabilities and situations.
3. Draft comprehensive user guides and solution walkthroughs for the challenges, assisting participants in their learning journey.
4. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team (IAM, client, projects).

Internship requirements

- Knowledge in programming and web development to build and maintain the CTF platform.
- Strong understanding of IAM concepts, common cyber vulnerabilities, and best practices.

Values

- Strong communication skills
- Eagerness to learn
- Creativity

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Leveraging AI to accelerate Access recertification process and assure compliance with DORA Regulation

Context

The Digital Operational Resilience Act (DORA) is a regulatory framework proposed by the European Commission to ensure that the financial sector in Europe maintains robust digital operational resilience. With the increasing complexity of IT systems and the rising number of cyber threats, financial institutions are required to undergo frequent access recertifications to comply with DORA standards. The recertification process can be time-consuming and resource-intensive. AI presents a promising solution to streamline and accelerate this process, thereby enhancing compliance efficiency and reducing operational risks.

Internship objectives

1. Develop a conceptual framework for integrating AI into the recertification workflow.
2. Propose AI-driven solutions for automating data collection, risk assessment, and reporting tasks.
3. Design and implement a pilot project to test the effectiveness of the AI-enhanced recertification process.
4. Collect and analyze data to measure improvements in speed, accuracy, and compliance rates.
5. Provide recommendations for scaling AI solutions across different financial institutions.

Internship requirements

- Proficiency in AI and machine learning techniques and tools.
- Experience with data analysis and statistical methods.
- Familiarity with programming languages such as Python or R.

Values

- Strong communication skills in English
- Eagerness to learn
- Self-motivated
- Teamplayer

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Onboarding SaaS applications onto IGA platforms by leveraging AI and RPA

Context

Introduction to the internship program focusing on the use of Artificial Intelligence (AI) and Robotic Process Automation (RPA) to automate the onboarding of Software as a Service (SaaS) applications into Identity Governance and Administration (IGA) tools. Emphasis on the importance of integrating AI with cybersecurity to enhance digital resilience in the financial sector, in line with the Digital Operational Resilience Act (DORA) regulations.
Seeking candidates with expertise in AI, RPA, machine learning, data analysis, and programming languages, who are also equipped with strong communication skills and a collaborative spirit.

Internship objectives

1. To understand the theoretical and practical aspects of AI and RPA in the context of cybersecurity and access management.
2. To develop user guides and solution frameworks for automating the onboarding process of SaaS applications into IGA tools.
3. To create a pilot project that demonstrates the effectiveness of AI and RPA in streamlining the onboarding process, improving speed, accuracy, and compliance.
4. To provide strategic recommendations for the implementation of AI-driven procedures in financial organizations.
5. A fully operational proof-of-concept that utilizes AI and RPA for the onboarding of SaaS applications into IGA tools.

Internship requirements

- Proficiency in AI and machine learning techniques and tools.
- Experience with data analysis and statistical methods.
- Familiarity with programming languages.

Values

- Strong communication skills in English
- Eagerness to learn
- Self-motivated
- Teamplayer

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Blue Team : Building Secure Cloud Components

Context

Cloud security is a niche which has seen enormous growth in the last few years. Given that businesses are increasingly migrating to the cloud, attackers are adapting and taking advantage of the misconfigurations often present in this type of environment. We need you to create secure cloud components (VMs, networks, storage solutions) to better protect cloud users.

Internship objectives

1. Research and understand the different concepts of cloud and cloud security.
2. Research on best practices, well-known issues and misconfigurations with popular cloud services
3. Create Infrastructure-as-Code (IaC) scripts to reduce vulnerability to data exposure, unauthorized access, and other security threats
4. Test and compare multiple IaC languages (Terraform, OpenTofu, ARM templates, ...) and their deployment methodologies

Internship requirements

- Knowledge of cybersecurity fundamentals
- A desire to learn new things

Values

- Motivated
- Professionalism
- Positive Attitude & Energy

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Cloud Security: Crafting Custom Azure Policies Used for Service Hardening and Compliance

Context

Are you ready to dive into the world of cloud security and make an impact? As an intern, you'll develop and implement custom Azure policies to harden cloud services, ensuring robust security for our clients. Document your innovative solutions and lead the charge in resolving and tracking non-compliances, all while gaining hands-on experience in the field of cloud security.

Internship objectives

1. Design and create custom Azure policies to improve the security of cloud services and govern security compliance and exception management
2. Acquire practical experience and deepen your knowledge in the evolving domain of cloud security and Azure policy implementation
3. Document hardening procedures and best practices for Azure services, producing detailed guides for client use
4. Work with the team to deliver specialized security solutions, enhancing client cloud security

Internship requirements

- Currently pursuing a degree in Computer Science, Cybersecurity, IT, ...
- Basic knowledge of cybersecurity principles and best practices
- Ability to document technical processes clearly and concisely

Values

- Enthusiasm for learning about cloud security and compliance
- Good communication skills, a proactive attitude, collaborative spirit
- Strong problem-solving abilities and attention to detail

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Building a Cloud "Capture the Flag" Platform

Context

Build an interactive environment to host "capture the flag" events for the Cloud Security team. It entails designing, building and optimizing the platform and potentially adding features to host multiple cloud-based "CTF" scenarios in a collaborative way.

Internship objectives

1. Analyze different approaches to build a cloud-based "CTF" platform that can be created and destroyed automatically, featuring CTF challenges in a Cloud Environment.
2. Work with a CICD mindset to build the platform using Azure pipelines
3. Design cloud challenges and implement them on the cloud-based "CTF" platform
4. Implement your solution and test it on a team of cloud experts

Internship requirements

- Build a cloud-based "CTF" platform
- Make at least one "CTF" scenario
- Report on your approach with a presentation

Values

- Is willing to continuously improve the platform
- Can work well in a collaborative environment
- Can tackle problems with an analytical approach

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Securing the architecture of a Cloud tenant

Context

At EY, we have built an automatic security tool (the CSI) to scan clients' clouds and list their potential misconfigurations & vulnerabilities. The tool is hosted on a cloud tenant which could use multiple security improvements.

Internship objectives

1. Understanding the Cloud Concepts + Cloud Security
2. Work with a CICD mindset to a production environment
3. Analyze the different security weaknesses of the cloud
4. Design a Solution and make a Remediation Plan
5. Implement the Remediation

Internship requirements

- Cyber security basics at least
- Cloud interest at least, Cloud knowledge is better
- Desktop Programming knowledge (e.g. Python)

Values

- Motivated
- Professionalism
- Positive Attitude and Energy

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Application Security extension for Azure DevOps

Context

The primary objective is to create an Azure DevOps pipeline results page/tab to consolidate all results from security testing/tooling. From a real world perspective, we see that developers struggle with the many tools within a big firm. This internship aims at a better developer experience for security like Spotify's Backstage framework. Your work will directly contribute to better serve our clients with new products.

Internship objectives

1. Analyze and investigate available Open-Source security tools (SAST, SCA, IAC)
2. Investigate which standard or formats can be used to export or save these results
3. Develop an attractive visual format to display these results
4. Understand the difficulties and caveats of vulnerability management
5. Bring your own ideas to the table to further extend functionality.

Internship requirements

- Interest and/or understanding of Azure DevOps and CI/CD pipelines.
- Familiarity or interest in code vulnerability scanning and cybersecurity principles.
- Coding experience in Python and Javascript/html for visualization.
- ELK / Kibana knowledge is a plus

Values

- Strong communication skills in English both written and spoken
- Proactive communication and knowledge sharing
- Eagerness to learn and adapt in a fast-paced technology environment

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Design and Implementation of Tabletop Exercises for Cybersecurity Incident Response

Context

Tabletop exercises are crucial tools for organizations to test and refine their incident response plans without the risks associated with live testing.
The exercises simulate various cybersecurity incidents, allowing teams to practice their response strategies, identify gaps in their procedures, and improve overall readiness.

Internship objectives

1. Design custom tabletop scenarios: Develop realistic and relevant cybersecurity incident scenarios (Ransomware, data breaches, insider threats, DDoS, etc.) that challenge different aspects of the incident response process.

2. Develop Exercise Materials: Create detailed documentation for each scenario, including incident timelines, injects (events or information provided during the exercise), roles and responsibilities, and expected outcomes.

3. Facilitate Tabletop exercise: Coordinate and conduct the tabletop exercises with relevant stakeholders, including IT staff, management, and external partners. Ensure that each participant understands their role and responsibilities within the exercise.

4. Create a template for future exercises: Develop a reusable template for future tabletop exercises that can be easily adapted to different scenarios and evolving cybersecurity threats.

Internship requirements

- Knowledge of common and new emergent threats
- Capability to think as an attacker and a defender

Values

- Strong English communication skills
- Ability to think critically about complex problems

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

Developing and Operationalizing Cyber Threat Intelligence for Proactive Defense

Context

Cyber Threat Intelligence (CTI) involves the collection, analysis, and dissemination of information about potential or ongoing threats to an organization's assets.
By leveraging CTI, organizations can proactively defend against emerging threats, understand the tactics, techniques, and procedures (TTPs) of adversaries, and improve their overall security posture.

Internship objectives

1. Perform threat landscape analysis using various sources of CTI including OSINT, commercial threat feeds, dark web monitoring, etc. and develop and share Intelligence reports focus on specific threats, actors, TTPs, or incidents.
2. Analyze the TTPs used by adversaries using frameworks like MITRE ATT&CK to map out how these TTPs and their defenses align with an organization security posture.
3. Investigate and implement a Threat Intelligence Platform (TIP) to centralize and manage the intelligence data. Understand how it can be implement with existing security tools such as SIEMs, Firewalls, IDS/IPS, etc to integrate it into the organization's security operations by creating rules or setting up IOCs.
4. Develop use cases where CTI can improve the organization's ability to detect, prevent, and respond to threats.
5. Ensure continuity and adaptation of the solution for continuous monitoring of the threat landscape and updating intelligence as new threats emerge and change daily

Internship requirements

- Knowledge of common and new emergent threats
- Familiarities with Threat Intelligence frameworks like MITRE ATT&CK

Values

- Strong English communication skills
- Ability to think critically about complex problems
- Proactivity attitude towards research and analysis

You can apply by sending your CV and preferred topic to katrien.de.neve@be.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

ey.com/be

EY
Building a better
working world