EY FSO Cyber Security

Internships 2023-2024

Building a better working world

Security Awareness – Cyber Board Game

Context

Security awareness programs for employees represent a vital pillar to maintain activities and reduce risk in a fast moving cyber threat landscape. Yet, capturing employees' attention remains a challenge. The application of game-like techniques to trainings yields to increased engagement and a smoother adoption of desired behaviors. The goal of the internship is to create a board game on the topic of cyber security to a general public.

Internship objectives

1. Research defined cyber security topics prompt to capture the attention of a general public.
2. Create a cohesive storyline and a branching scenario for the cyber board game.
3. Draft the game cards and flesh out the game possibilities; humor and wit are more than welcome!
4. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team.

Internship requirements

- Intern should have interest in cyber security
- Intern should have some experience in game scenario development
- Intern should be able to create an immersive experience

Values

- Intern must be able to work independently, with support of mentor
- Creativity and imagination
- Strong communication skills in English

Security Awareness – AI Awareness

Context

Lately, we have seen generative AI and ChatGPT gain remarkable significance. As we navigate the intricate landscape of AI-driven innovations, it's imperative to cultivate awareness about secure practices and the potential for AI-related fraud. This cybersecurity internship focuses on creating solutions towards general end-users about responsible AI usage, potential risks, and secure behaviors.

Internship objectives

1. Research the topic of AI, natural language processing and ChatGPT and create an overview of associated risks, including data privacy, bias, misinformation, fraud, and potential misuse.
2. Develop a structured security awareness curriculum by listing learning objectives and secure behaviors that end users should be made aware about.
3. Brainstorm ideas of optimal and innovative awareness solution to convey the topic to the end-users in an engaging manner.
4. Create real-life case studies and practical exercises.
5. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team.

Internship requirements

- Intern should have interest in cyber security and AI

Values

- Intern must be able to work independently, with support of mentor
- Analytical skills
- Strong communication skills
- Willingness to learn

Security Awareness - Escape Room

Context

Security awareness programs for employees represent a vital pillar to maintain activities and reduce risk in a fast moving cyber threat landscape. Yet, capturing employees' attention remains a challenge. The application of game-like techniques to trainings yields to increased engagement and a smoother adoption of desired behaviors. The goal of the internship is to create an escape room scenario related to cyber security.

Internship objectives

1. Imagine an escape room scenario for the subject of cyber security.
2. Create and test cues and challenges to be incorporated in the escape room scenario based on own research.
3. Flesh out the scenario and select relevant material objects and items, in order to "set the scene" and obtain an immersive experience for the participant.
4. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team.

Internship requirements

- Intern should have interest in cyber security
- Intern should have interest in board games or escape rooms
- Intern should be able to create an immersive experience

Values

- Intern must be able to work independently, with support of mentor
- Creativity and imagination
- Willingness to learn

Security Awareness – Phishing Identification Chatbot

Context

Security awareness programs for employees represent a vital pillar to maintain activities and reduce risk in a fast moving cyber threat landscape. Yet, capturing employees' attention remains a challenge. The application of game-like techniques to trainings yields to increased engagement and a smoother adoption of desired behaviors. The goal of the internship is to create a gamified decision tree to identify a potential phishing mail under a dynamic chatbot format.

Internship objectives

1. Research recommendations and secure behaviors to identify phishing.
2. Rewrite a dynamic 'decision tree' chatbot scenario following a branching scenario.
3. Benchmark the chatbot on different scenarios.
4. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team.

Internship requirements

- Intern should have interest in information security awareness
- Intern should have some knowledge in programming
- Intern should have interest in Machine Learning (ML)

Values

- Intern must be able to work independently, with support of mentor
- Creativity
- Strong communication skills in English

Cloud Security Control Framework

Context

Cloud security is a niche which has seen enormous growth in the last few years. As enterprises are migrating their applications to the cloud, new vulnerabilities and exploits become available. Without a cloud security framework, organizations lack the in-depth visibility needed to determine if their data is adequately secured.

Internship objectives

1. Research and understand the different concepts of cloud and cloud security.
2. Research on best practices, existing frameworks, well-known issues, etc.
3. Create a cloud security framework to reduce vulnerability to data exposure, unauthorized access, and other security threats.
4. Make the framework as complete as possible to cover the most scenarios, the most security threats and the most CSPs (Azure, GCP, AWS).
5. Integrate the framework into our Cloud Security Assessment tool.

Internship requirements

- Knowledge and experience with security concepts
- Intern should have a good understanding of the cloud

Values

- Intern must be able to work independently
- Intern must be fluent in English
- Intern should have a consultant mindset

Build the Ultimate Microsoft 365 Security Assessment Framework

Context

In our interconnected world, safeguarding organizational data from cyber threats is crucial. This internship offers a chance to explore cloud security and Microsoft 365 security. Gain hands-on experience in using Microsoft's security features to defend against threats like phishing, ransomware, malware and email compromise. Finally, build a framework to assess Microsoft 365 security.

Internship objectives

1. Acquire knowledge on foundational cloud concepts, with a specific focus on Azure and its security aspects.
2. Gain insights into new offensive techniques targeting Microsoft 365 services. Understanding attackers' methodologies equips you to swiftly identify and counteract malicious activities, ultimately enhancing defensive capabilities.
3. Investigate Microsoft services to protect 365 such as Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Purview, etc.
4. Discover and experiment with Open-Source tools for 365 Security assessments.
5. Use the knowledge you've gained to construct a comprehensive framework for evaluating 365 security.

Internship requirements

- Solid understanding of cybersecurity fundamentals
- Strong interest in cloud and cloud security
- Analytical mindset

Values

- Motivated
- Professionalism
- Positive Attitude and Energy

Contribute to EY's Cloud Security Posture Management (CSPM) Assessment Tool

Context

Organizations increasingly migrate their services to cloud environments. Therefore, the need for robust cloud security becomes indispensable. EY has developed a cloud security tool aimed at evaluating the security posture of cloud environments. To further enhance the effectiveness and scope of this tool, we are offering an internship for a student to join our team and contribute to the advancement of cloud security.

Internship objectives

1. Ensure the cloud security tool's maintenance, functionality and alignment with latest security standards.
2. Expand the tool's offensive and defensive scanning features, using new techniques to simulate real-world cloud attacks.
3. Craft clear data visualization dashboards to offer complex security insights on findings in cloud environments.
4. Contribute to building a versatile cloud security toolbox, which comprises offensive and defensive tools to assess cloud environments.
5. The aim for you is to have the opportunity to integrate your internship work into an EY cloud assessment application. This practical experience will allow you to see the direct impact of your contributions on real-world projects.

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

Automate OSINT Data Collection of Cloud Environments

Context

With the rapid adoption of cloud technologies, ensuring robust cybersecurity measures is a must. This internship aims to automate OSINT data collection for cloud environments, addressing emerging threats and contributing to the security of modern businesses.

Internship objectives

1. Discover the Power of Open Source Intelligence (OSINT). Gain a solid understanding of how to gather valuable information from publicly available sources.
2. Find powerful tools and techniques tailored for OSINT data collection in cloud environments.
3. Learn how to use them. Start with small-scale projects, to finally use OSINT tools and extract meaningful insights on any cloud environment automatically.
4. Learn how to present all your findings in a way that aligns with business needs and facilitates decision-making.
5. If time permits it, the aim for you is to have the opportunity to integrate your internship work into an EY cloud assessment application. This practical experience will allow you to see the direct impact of your contributions on real-world projects.

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

Iaas Project MS Azure – ISO Compliance

Context

The core aim is to create a fully automated cloud environment for our technical teams, customizable using tools such as Terraform and Ansible. The foundation has been established but the ultimate objective is to ensure ISO 27001 compliance for this environment, bolstering its marketability.

Internship objectives

1. Learn the current setup and identify ISO 27K gaps.
2. Create code changes to make the environment ISO compliant.
3. Keep security and usability in mind.
4. Create Dashboarding to follow-up ISO compliance rate.
5. Free to request your own idea's that could make the difference.

Internship requirements

- Interested / experience with IAAS products
- Basic Knowledge of Terraform and Ansible
- Basic knowledge of ISO 27k
- Strong documentation skills

Values

- Security minded
- Eager to learn
- Teamplayer

Creation of a Penetration Test Report Solution

Context

The reporting is always the less exciting phase of a penetration test. Create a solution that automates the creation of a penetration test report to improve productivity and quality, and reduce human errors.

Internship objectives

1. Build a solution that can be used to automate the creation of penetration test reports.
2. Develop a solution including a web interface and a database to store evidences and automatically fill in a report template based on the penetration tester input.
3. The solution should be intuitive, flexible and easy to maintain.
4. Implement a way for people to easily collaboratively contribute to reports and the knowledge database.
5. The solution would ideally be hosted in Microsoft Azure.

Internship requirements

- Strong development skills. Experience with automatic deployment is a plus
- Being security-minded for securely developing the solution
- Basic understanding of cloud solutions and cyber vulnerabilities

Values

- Being able to work independently with support of mentor
- Having a consultant mindset
- Decent mastery of English, both writing and speaking

Purple Team Methodology

Context

In order to continually evaluate their resilience against cyber threats, companies regularly engage in purple team exercises. To correctly assess any potential flaws, the organization of these exercises has to be thoroughly planned and executed.

Internship objectives

1. Research known frameworks, methodologies, and standards.
2. Research on tools and processes to efficiently communicate findings between the red and the blue team.
3. Research on identifying critical functions within a network, and linking relevant Purple Team exercises.
4. Implement findings in EY's methodology.

Internship requirements

- Technical knowledge of security testing
- Intern should have a good understanding Purple Teaming

Values

- Intern must be able to work independently
- Intern must be fluent in English
- Intern should have a consultant mindset

Antivirus Development

Context

Antivirus solutions are omnipresent in the cybersecurity landscape. Research the different types of antiviruses and their working. Based on the results, develop your own antivirus solution and compare it against others by testing it with malicious files. Write a comprehensive conclusion about antivirus technology based on what you have tested.

Internship objectives

1. Develop your own antivirus.
2. Understand the different types of detection.
3. Test the antivirus out on malicious files.
4. Compare the detection rate to other antiviruses.
5. Write conclusions on antivirus technology & what you have tested.

Internship requirements

- Strong English skills
- Knowledge of programming languages
- Logical thinking

Values

- Autonomy
- Competency
- Determination

Evaluating the Effectiveness of Adaptive Authentication Protocols (IAM)

Context

In an increasingly digital world, ensuring both robust security and seamless user experiences is paramount. Our research delves into the realm of adaptive authentication protocols, a dynamic approach that tailors security measures based on contextual factors. As aspiring researchers, you'll explore a spectrum of adaptive methods—risk-based, behavior-based, and context-based authentication—to evaluate their effectiveness in thwarting threats while minimizing user friction. Uncover the intricate balance between security and user convenience, and contribute to enhancing the landscape of modern cybersecurity

Internship objectives

1. Compare the performance of different adaptive authentication methods in real-world scenarios
2. Evaluate how different adaptive methods impact user experience.
3. Measure the actual security improvements offered by adaptive authentication.
4. Identify potential vulnerabilities or limitations in adaptive authentication methods
5. Apply your research to various sectors.

Internship requirements

- A basic grasp of cybersecurity concepts, especially as they relate to IAM.
- Ability to conduct a thorough literature review to understand existing adaptive authentication methods, their strengths, weaknesses, and any gaps in current research.

Values

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

The Role of IAM in Bridging Business & IT Strategies

Context

Identity & Access Management (IAM) serves as a critical juncture between business operations and IT security. A robust IAM methodology not only ensures technical proficiency but also aligns with business goals, regulatory requirements, and user experience. It forms the backbone of an organization's cybersecurity strategy, balancing risk management with operational efficiency. Students undertaking this internship will dive into the intricate world of IAM, crafting methodologies that synchronize business imperatives with cutting-edge cybersecurity practices. Participating in this internship will equip students with a comprehensive understanding of IAM's strategic role, bridging the gap between business goals and cybersecurity imperatives.

Internship objectives

1. Conduct interviews and workshops with both technical and business stakeholders to understand their needs, challenges, and objectives related to IAM.
2. Study best practices in IAM methodology from industry leaders and standards bodies to ensure the proposed methodology is both innovative and grounded.
3. Construct a comprehensive IAM methodology document that addresses business goals, user experience, security requirements, and regulatory compliance.
4. Develop a phased approach for implementing the IAM methodology, including metrics to measure its effectiveness
5. Implement findings in EY's Methodology

Internship requirements

- A foundational grasp of IAM concepts and their relevance to business operations and compliance.
- Strong understanding of business processes, goals, and the strategic role of IT in achieving them
- Ability to seek out, evaluate, and integrate industry best practices and standards into the methodology

Values

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

IAM Capture the Flag Platform

Context

CTF competitions are gamified environments designed to challenge and train cybersecurity professionals on real-world scenarios. Given the vital role IAM plays in safeguarding digital identities, a CTF focused on IAM presents a unique opportunity to highlight its nuances and complexities. Developing a robust IAM-centric CTF platform would not only elevate the cybersecurity community's understanding of IAM challenges but also foster innovation and solutions in this domain. Engaging in this internship will equip students with a unique blend of technical development skills and a deep understanding of IAM, paving the way for a promising future in cybersecurity.

Internship objectives

1. Create realistic IAM challenges that mimic real-world vulnerabilities and situations.
2. Develop a scalable and user-friendly platform to host the IAM challenges, ensuring a seamless experience for participants.
3. Implement a robust scoring system to gauge participant performance, and a leaderboard to foster competition.
4. Draft comprehensive user guides and solution walkthroughs for the challenges, assisting participants in their learning journey.
5. As a proof-of-concept, test the final deliverable with the EY FSO Cyber Team

Internship requirements

- Proficiency in programming and web development to build and maintain the CTF platform.
- Ability to craft challenging and diverse IAM scenarios that can engage a wide range of participants.
- Strong understanding of IAM concepts, common vulnerabilities, and best practices.

Values

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

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