It takes one, to know one

Introduction

The rapid growth of implementing and using Information Technology in current businesses expose companies and their customers to several inherent risks. Management and company's boards have identified managing security risks as being of strategic importance. These risks include, not only possible leakage of confidential, strategic and intellectual property data, but also compliance aspects for running businesses. While companies are exposed to these types of security risks, security experts and ethical hackers are becoming scarcer than ever! In order to cope with the expansion of complex IT, security challenges and the rapidly growing demand for IT security testing (penetration testing), we prosed to develop expert systems, techniques and algorithms to automatically learn from the smartest and most skilled (ethical) hackers on a continuous base and to applied learned knowledge in the execution of the next generation security tests.

Relevant questions that can be usage as basis for academic research are:

- **Understand the expert** – Analyze the methods, thinking, tools and techniques our ethical hackers are using to execute advanced security testing.
- **Identify prior knowledge** - Understand what data and information can be used as prior knowledge for our expert systems. This includes, but is not limited to; output from vulnerabilities scanners, available threat intelligence data, intrusion detection and security incidents from Security Information and Event Management (SIEM).
- **Identify relevant data for mining purposes** - Understand what data sources, event loggers and hackers tooling can function as relevant data input for creating data models and machine learning algorithms to predict potential attacks that might be happening. These data sources include, but are not limited to; proxy servers' logs, web server's logs, data bases logs, switches, routers logs and (application) firewall logs.
- **Model, learn and supervise expert systems** - Create, learn and supervise models to predict potential attacks that might be happening based data from the identified relevant sources (see previous questions). Machine learning models to be used includes, but are not limited to neural networks, decision trees, clustering, association rules, reinforcement learning etc.

Tools

We have many advanced tools available, such as R, Qlikview, SAS, Orange, SQL, Weka, etc.

Profile

For this internship we're looking for someone with the following profile:

- You are in the final stages of your master in Computing Science, Information Security, Artificial Intelligence, Mathematics, Econometrics or related programs;
- You have some experience with the described techniques, and are a rapid learner;
- You are analytically strong, have a strong focus on achieving results and have a good eye for quality;
- You have affinity with both Data Analytics and Cyber Security.

What do we offer?

We offer an internship with the Data Analytics team, in cooperation with the Security team. There is an open and professional corporate culture with a lot of room for innovation and personal initiatives. There is a good work-life balance, and there are a lot of initiatives to get to know each other better outside of work.

During your internship you get assigned a counselor, with whom you will discuss the progress of your research periodically. Of course, the rest of the team is also available for discussion if you run into some issues. You will receive a market-oriented salary and a laptop.

Why Deloitte

Deloitte has a strong and large hackers group that will support in the research by among others generating relevant data sources and use-cases trails and making these available for further research. Deloitte's Analytics practice is also growing rapidly and security analytics is identified as the next growth area. This research will be focused on bringing these two competence, security testing and analytics, together to create value to Deloitte's security propositions and ultimately to Deloitte's clients.

Report from Kennedy:
"Deloitte is heavily investing in analytics and plans to embed analytics offerings throughout all service areas on a global basis. In order to take analytics to market, the firm has formed a Center of Excellence called the Deloitte Analytics Institute (DAI). The DAI enables employees to share and leverage thought leadership, methods, tools, and solutions around the globe."

Deloitte has extensive experience in the field of advising and assessing the information security within governments and business. Our team consists of more than 35 specialists that describe "ethical hacking" as their great passion. The knowledge, experience and passion is reaffirmed in the recent finals of the Global CyberLympics. The team of Deloitte Netherlands did win, for the third time in a row a contest which consisted of both offensive and defensive security challenges.

Contact

Are you interested in this position? Contact us today!

If this internship doesn't fit your profile, but you do know someone who would be perfect for it, please pass this internship offer along.

For questions about this internship, please contact Liselotte Mulder (LMulder@deloitte.nl or +31882883616) or Irfaan Santoe (ISantoe@deloitte.nl or +31882886012).