EXCELLIUM

Cyber Solutions by Thales

CERT-XLM Computer Security Incident Response Team

Internships 2023-2024

Latest update: 2023-09-12

SCAN ME!

Contents

1 Introduction

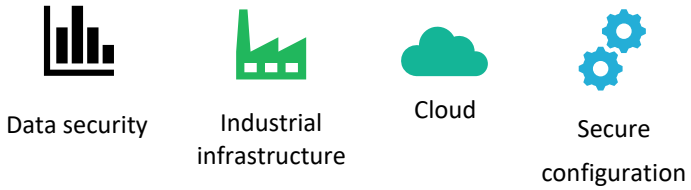
1.1 Excellium Cyber Solutions by Thales

Excellium Cyber Solutions by Thales is a cyber-security consulting and technology Integration Company established since 2012 in Luxemburg and Belgium, with activities worldwide. The group employs over 200 people acting exclusively in the information security domain.

1.2 What can we do?

1.2.1 Advisory Services

1.2.2 Cybersecurity Infrastructure



1.2.3 Managed Detection and Response

Cyber Security Operation Center
CSOC

- SOC as a Service
- SOC customer
- 24/7 monitoring
- Vulnerability Scans
- DDoS testing
- EDR as a Service

Computer Security Incident Response
CERT-XLM

- Threat Intelligence detection and response
- DFIR
- Vulnerability Management
- Digital surveillance

1.2.4 Test, Adapt And Prevent

- Red teaming
- Penetration Testing
- Application testing/code review
- Threat Intelligence Reports

2 CSIRT Team

CERT-XLM it the incident response team of Excellium Services. Our goal is to improve and help companies during Cyber incidents. The CERT-XLM is an established CSIRT since 2014. It is an certified team of TF-CSIRT Trusted Introducer, First.ORG and member of the CERT.LU and CyberCoalition.be initiative. CERT-XLM has performed more than 700 incident handlings since its creation.

Our main mission is DFIR (Digital Forensic). However additionally to this, we develop and maintain tools to improve the monitoring of the external surface of our customer (typo squatting detection, intrusion detection use case, threat intelligence integration, digital surveillance….)

Structured catalogue of services

- DFIR (Breach analysis, Doubt removal)
- IR exercices
- Trainings

Certified and screened professionals

- Certifications from GIAC (SANS)

Field experience

- More than 60 Incident managed yearly
- Certification of the team.
- Clients in all industries
  (banking and insurance, energy,
  transportation, healthcare, education…)

3 Internships

3.1 Introduction

Are you passionate about cybersecurity and eager to make a significant impact in the world of penetration testing and/or application security?

We offer exciting internship opportunities where you'll immerse yourself in team of experienced consultants.

Have a look to our list internship topics you can choose from. 😉

Position: IT Security Intern 👩‍🦱👨‍🦱

Duration: 4 to 6 months

Locations

Excellium Services S.A.

5 rue Goell

L-5326 Contern, **Luxembourg**

Excellium Services Belgium N.V.

Orion Bldg, Belgicastraat 13

B-1930 Zaventem, **Belgium**

Send your application to

recruitment@excellium-services.lu

recruitment@excellium-services.be

3.2 Recruitment process

1) **Pick your 3 favourite internships subjects** that you find the most relevant with your experience and your motivation, you can also BYOS, or "Bring Your Own Subject". 😉

2) **Contact our Human Resources department** (either in Belgium or Luxembourg). Send them your CV, tell them about the subjects you like and why you think you would be a good candidate for them. Give us also details about the expected duration of your internship and the period. The interview could have parts in French, English and Dutch, depending on the languages indicated in your CV.

   Our priority is to onboard our trainees as full time employees in the team after their internship. However, we are open to propose our trainings for students that are in the middle of their scholarship (if it's not their final internship).

3) **Solve our challenge.** We will give you a small coding challenge to solve. We estimate that the challenge requires a few hours to solve. We are open to give you hints if you are stuck with the challenge. Let us know what you tried and we will be happy to help and check that everything is working properly.

4) **Send us a your code and a small recap, redacted in English**, that describes your approach to solve the challenge. Depending on the challenge, we may also request recommendations or remediation steps. This will be clearly stated if this is the case.

5) **Do a technical interview with the Team Leader or the Team Leader's deputy.** This is last step of our recruitment process. We will discuss with you during about 1h00 and 1h30 about your school, personal and professional experiences. We are interested by what makes you motivated and passionate about IT and IT security. Tell us about any personal project (including personal sites, scripting, tools, "IT @ Home", home automation…), contribution to open source projects, participation in CTF (either as a player or challenge creator…), participation in IT Security groups, bug bounties, CVE…

6) **We will review the different applications and propose an internship to the best candidates.** First applications (and first resolutions of the challenge) will be considered by priority.
   We may also propose internships for our other departments as alternative if we cannot accommodate all candidates. All our internships at Excellium are exclusively related to IT Security.

4 Subjects

4.1 CDN / Virtual host detection

📖 Description

Excellium Services offers an internship opportunity within our company in the CSIRT team. This internship focuses on the detection of CDN (Content Delivery Network) and Virtual Hosts in a PDNS (Passive DNS) dataset.

Before diving into the details of this project, it's essential to understand the key concepts.

A CDN, or Content Delivery Network, is a network of geographically distributed servers designed to distribute Internet content, such as images, video, and static data, to end users quickly and efficiently. CDNs are used to improve website loading speed and content availability by delivering content from servers close to users.

On the other hand, PDNS, or Passive DNS, is a database that passively records DNS queries made on a network. It stores information on domain names and associated IP addresses, making it a valuable source of data for IT security.

The aim of this internship will be to develop techniques for detecting and scoring IPs linked to CDNs or Virtual hosts within PDNS data. This task is crucial to the successful implementation of Threat Intel, as unvalidated CDN IPs can generate numerous unnecessary alerts (false positives), complicating the tracking of real threats.

You will have the opportunity to work on exploring data analysis techniques, and contribute to improving our detection infrastructure.

This internship will enable you to develop valuable cybersecurity skills, work with experienced professionals and make a significant contribution to our mission of strengthening the company's security. If you are passionate about IT security and would like to take up this stimulating challenge.

🎯 Objectives

- On prem data lake analysis
- Time constraint analysis
- Study how to detect false positive candidates
- Manage from development to production

💻 Skills Involved

- **Backend Development**: Integration through API to the current Threat Intelligence.
- **Coding**: Being able to write python code
- **System**: Understanding system and be able to deploy the application in both UAT and production.
- **Cybersecurity Awareness**: Understanding the Threat Intelligence and CSOC need

4.2 Parking and dormant website detection

📖 Description

Excellium Services is delighted to offer you an internship opportunity within our company, as part of the CSIRT (Computer Security Incident Response Team). We have a challenge waiting for you: the automated detection of parked or inactive sites. This mission is essential to automate and reduce manual actions in our detection system, and we'd like to develop a Machine Learning-based algorithm to achieve this.

Detecting automatically these inactive sites is crucial to strengthening our arsenal in the fight against typosquatting and phishing. Automating this process will enable us to increase efficiency and better protect our customers against online threats. You will have the opportunity to work with our team, learn the ins and outs of Machine Learning applied to cybersecurity, and contribute to a fundamental mission: protecting data and privacy online.

This internship will enable you to develop valuable cybersecurity skills, work with experienced professionals and make a significant contribution to our mission of strengthening corporate security. If you are passionate about IT security and would like to take up this stimulating challenge.

🎯 Objectives

- Improve current digital surveillance operation by automatising detection of dormant websites.
- Use machine learning to resolve challenging detections scenario.
- Improve human productivity.

💻 Skills Involved

- **Backend Development**: Integration through API to the current Threat Intelligence.
- **Coding**: Being able to write python code
- **Machine Learning**: Understand and being able to use machine learning techniques.
- **System**: Understanding system and be able to deploy the application in both UAT and production.
- **Cybersecurity Awareness**: Understanding the Threat Intelligence and CSOC need

4.3 Creation of scored Passive BGP AS Database

📖 Description

Excellium has a rich source of telemetry data, including passive DNS records. This data provides valuable information on the correspondence between host names and IP addresses at any given time. However, it is essential to note that IP addresses are dynamic and changeable. In networking terms, an Autonomous System (AS) represents a set of computer networks under the control of a single entity, such as an ISP, end customer or transit provider. To accurately assess the potentially dangerous nature of an IP address, it is necessary to take into account the associated IP address ranges and, by extension, BGP ASes as a whole and their evolution over time.

The proposed project consists in studying and setting up a database that will be fed with information collected thanks to Excellium's passive DNS telemetry. This database will be used as a passive resource for Autonomous Systems (AS) BGP. Project participants will also have to take into account the imperatives and constraints inherent in processing large quantities of data. One of the project's final objectives will be to develop an AS scoring system based on the information available in the Threat Intelligence database.

This project has several innovative aspects:

- Over and above technical development, it offers students the opportunity to explore issues related to intrusion detection and evidence gathering in the context of cybersecurity.

- It allows students to work with data in real time, giving them hands-on experience of managing constantly evolving data.

- Participants will have the opportunity to contribute to the creation of a valuable resource for IT security by analyzing BGP AS behaviors and developing a scoring system based on Threat Intelligence information.

This internship research project offers an exciting opportunity to explore key areas of IT security while developing technical skills and participating in the creation of a valuable database. Candidates will be encouraged to tackle technical challenges while learning about real network security issues, including the implementation of an innovative scoring system to assess the potential threat of BGP AS.

💻 Skills Involved

- **Backend Development**: Integration through API to the current Threat Intelligence.
- **Coding**: Being able to write python code
- **System**: Understanding system and be able to deploy the application in both UAT and production.
- **Internet routing**: Understanding the principles of Internet routing.
- **Database**: Design and management of a database adapted to the storage of BGP AS information.
- **Python**: Use of Python for data processing and analysis.
- **Digital processing**: Implementation of processing methods to extract relevant information.
- **Cybersecurity Awareness**: Understanding the Threat Intelligence and CSOC need

5 Career Opportunities

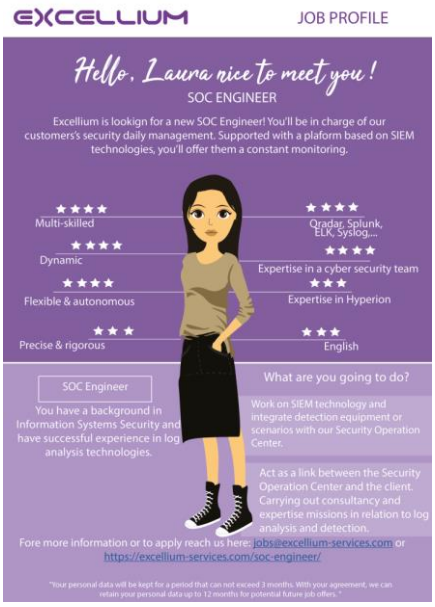
We offer opportunities for growth and development.

Your internship at Excellium can lead you to a job offer.

This is a chance to join an established consulting firm and work with leaders in your field to develop insight, experience and truly add value.

If you are striving to be the best, we want you!

Have a look at some of our job opportunities at Excellium?



More career opportunities at https://excellium-services.com/career-opportunities/