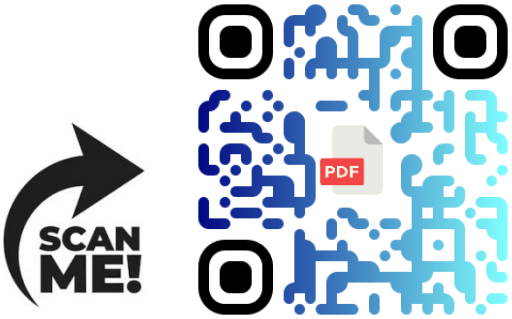
EXCELLIUM

Cyber Solutions by Thales

Information Security Governance

Internships 2023-2024

Latest update: 2023-09-26



Contents

1 Introduction

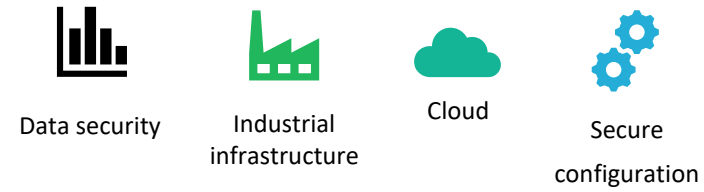
1.1 Excellium Cyber Solutions by Thales

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

Computer Security Incident Response
CERT-XLM

- EDR as a Service
- Threat Intelligence detection and response
- DFIR
- Vulnerability Management

1.2.4 Test, Adapt and Prevent

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

2 Information Security Governance Team

The Information Security Governance department is considered the cornerstone of our services and the diversity of expertise that Excellium has.

Indeed, having a transversal vision of all areas of information security, ISG supports our clients as a conductor of security initiatives.

The diversity of skills within ISG allows us to support our clients in:

- Establishing their security strategy and defining their information security program (projects, budget, roadmap).
- Improve resilience, including cyber incident management and response, BCP/DRP and crisis management.
- Design and structure the information security governance framework within an organization, including defining security policies and security processes ranging from vendor management to vulnerability management.
- Information security risk management (qualitative and quantitative).
- Assume the role of Chief Security Officer (CISO) within the organization or support a current CISO in their management of daily activities.
- Carrying out maturity assessments or information security audits against regulations/laws (DORA, NIS 2, CSSF circulars, etc.), standards (ISO/IEC 27001, etc.) or benchmarks (NIST CSF, SANS CIS, SWIFT CSCF, etc.).
- Training and awareness.
- Security advisory for a defined topic (e.g., cloud security or data protection).
- Operational security activities (e.g., risk-based vulnerability management).

With ~25 consultants, the ISG team is a leader business unit in the market.

3 Internships

3.1 Introduction

Are you passionate about cybersecurity and eager to make a significant impact in the world of governance?

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: ISG Consultant trainee

Duration: 4 to 6 months

Locations

Excellium Services S.A.

5 rue Goell

L-5326 Contern, **Luxembourg**

Excellium Services Belgium S.A.

Belgicastraat 13/1

B-1930 Zaventem, **Belgium**

Send your application to a unique address for **Belgium** and **Luxembourg**

recruitment@excellium-services.lu

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) **Do a technical interview with a member of the ISG team.** 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 cybersecurity, IT and IT security. Tell us about any personal project (including personal projects, "IT @ Home", home automation…), contribution to open-source projects, participation in IT Security groups, etc.

4) **We will review the different applications and propose an internship to the best candidates.**
   First applications 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 cybersecurity.

4 Subjects

4.1 Cyber Resilience

📖 Description and 🎯 Objectives

As part of a development center around resilience, your mission will consist of participating in the definition and implementation of approaches, tools and documents with the aim of:

- ❖ Improve the methodology and tools used to carry out business impact analysis as well as approach for defining a business continuity strategy and creating documents supporting this strategy (BCP plan, etc.) and fir defining a disaster recovery strategy and creating documents supporting this strategy (DRP plan, specific recovery procedures, etc.).
- ❖ Improve the existing approach and documents (methodologies, procedures, reflex sheets) on responding to security incidents.
- ❖ Improve the existing documentation on cyber crisis and communication, including the creation of scenario for cyber crisis simulation exercise.
- ❖ Participate as an observer in missions around resilience to identify areas for improvement and promote learning of the topics.

💻 Skills Involved

- **Business Continuity Management**: Being able to understand business consequence and having a holistic view of business processes to design relevant plans.
- **Incident Management**: Being able to understand incident impact and how to adequately respond to minimize the effects of the incident.
- **Crisis Management**: Being able to understand key pillars on crisis management and having creativity for the creation of scenario.

Context

The internship will take place at our premises in Contern, Luxembourg, in a dynamic environment with consultants specializing in the methodologies used and the relevant standards. The team in which the student will be integrated is called “Information Security Governance” and aims to provide our clients with expertise to establish a governance framework for information security for clients.

As the student gains autonomy, he will be encouraged to actively participate in our clients' projects if they are related to his internship, which will facilitate possible hiring.

Profile of the trainee

Curious student, autonomous but also capable of organizing team work, capable of understanding topics around information security by gaining perspective on it, creative and voluntary. Involved with a strong desire to learn and discover all facets of the profession.

Strong desire to understand and work on resilience concepts.

4.2 Vulnerability Management and Hardening

📖 Description and 🎯 Objectives

As part of a development center around vulnerability management, your mission will consist of participating in the definition and implementation of approaches, tools and documents with the aim of:

- ❖ Improve the methodology and security tools used to perform risk based vulnerability management. Security tools include Qualys, Tenable and any other vulnerability management tool.
- ❖ Support the consultants for the creation of presentation on vulnerability management and hardening.
- ❖ Participate in the creation of a service and the improvement of our capabilities for compliance check regarding hardening rules.
- ❖ Create specific templates for hardening rules based on best practices.
- ❖ Participate as an observer in missions around vulnerability management and hardening to identify areas for improvement and promote learning of the topics.
- ❖

💻 Skills Involved

- **Vulnerability Management**: Being able to understand the concepts of vulnerability management from the identification to the treatment, especially the assessment phase.
- **Hardening and Configuration Management**: Being able to understand the concepts of hardening and configuration, from the definition of the security baselines to the compliance checks of the devices.

Context

The internship will take place at our premises in Contern, Luxembourg, in a dynamic environment with consultants specializing in the methodologies used and the relevant standards. The team in which the student will be integrated is called “Information Security Governance” and aims to provide our clients with expertise to establish a governance framework for information security for clients.

As the student gains autonomy, he will be encouraged to actively participate in our clients' projects if they are related to his internship, which will facilitate possible hiring.

Profile of the trainee

Curious student, autonomous but also capable of organizing team work, capable of understanding topics around information security by gaining perspective on it, creative and voluntary. Involved with a strong desire to learn and discover all facets of the profession.

Strong desire to work on operational security topics, but with the governance point of view.

4.3 Risk Management and Assessment

📖 Description and 🎯 Objectives

As part of a development center around risk management, your mission will consist of participating in the definition and implementation of approaches, tools and documents with the aim of:

- Improve the methodology and tools used to perform qualitative risk assessment, including cyber risk scenario design, maturity level of security controls automation, libraries, etc..
- Improve the methodology and tool integration (Citalid) used to perform quantitative risk assessment, including potential losses definition and estimation.
- Participate in the creation of security frameworks and reports used for assessments.
- Participate as an observer in missions around risk management and assessment to identify areas for improvement and promote learning of the topics.

💻 Skills Involved

- **Risk Management**: Being able to understand the concepts of risk management, including qualitative and quantitative models (ISO 27005, EBIOS RM, FAIR methodology, etc.).
- **Cybersecurity Assessment**: Being able to understand the concepts of cybersecurity assessments, including the maturity model for scoring an organization regarding security domains.

Context

The internship will take place at our premises in Contern, Luxembourg, in a dynamic environment with consultants specializing in the methodologies used and the relevant standards. The team in which the student will be integrated is called “Information Security Governance” and aims to provide our clients with expertise to establish a governance framework for information security for clients.

As the student gains autonomy, he will be encouraged to actively participate in our clients' projects if they are related to his internship, which will facilitate possible hiring.

Profile of the trainee

Curious student, autonomous but also capable of organizing team work, capable of understanding topics around information security by gaining perspective on it, creative and voluntary. Involved with a strong desire to learn and discover all facets of the profession.

Strong desire to work on risk management as well as assessments and audits.

4.4 Your choice

💭 You have another topic in mind related to information security governance and would like to explore it here at Excellium?

Feel free to tell us about and we'll see what we can do!

5 Career Opportunities

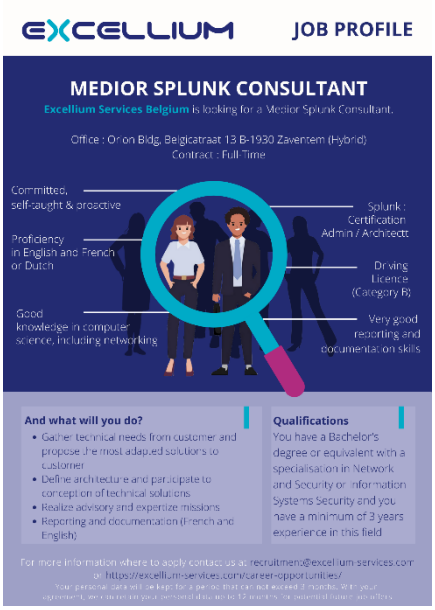
We offer opportunities for growth and development.

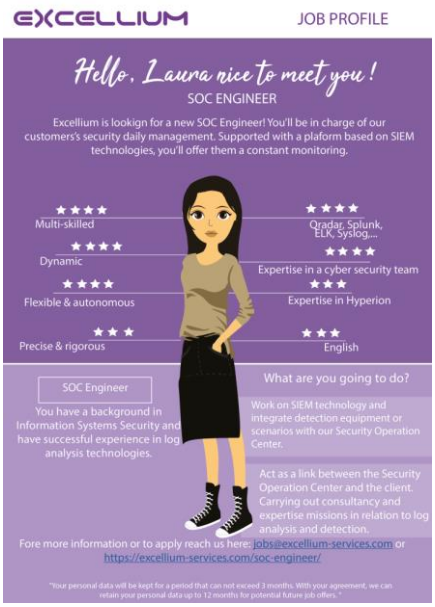
Your internship at Excellium can lead you to a job offer.

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/