Guylian De Wit

LL.M. (KU Leuven) · Advanced LL.M. candidate in IP & ICT Law · Former ethical hacker

CONTACT

Location
Belgium

E-mail
guylian@guylian.info

Website
guylian.info

LinkedIn
linkedin.com/in/guylian-d

GitHub
github.com/SpengeSec

LANGUAGES

Dutch	Native
English	Full professional
French	Fluent in conversation
Russian	Elementary (CEFR A1)

LEGAL FOCUS

- GDPR
- International data transfers
- NIS2
- Cyber Resilience Act
- Data breaches
- IT contracts
- EU law

TECHNICAL SKILLS

Security

Penetration testing · Web application security · Cloud security · Active Directory · Vulnerability research · OSINT

Programming & systems

Python · JavaScript · Bash · Linux · Networking (TCP/IP)

PROFILE

Law graduate specialising in data protection, cybersecurity and IT law, with several years of hands-on experience in offensive security as an independent security researcher and as a professional ethical hacker. I discovered a zero-day vulnerability (CVE-2019-19699), responsibly disclosed vulnerabilities to organisations such as the University of Cambridge and the U.S. Department of Defense, and carried out penetration tests for clients. My legal research focuses on EU data protection, international data transfers and data sovereignty.

EDUCATION

2026 – 2027 (expected)

Advanced Master of IP and ICT Law (LL.M.), *KU Leuven, Brussels*
Centre for IT & IP Law (CiTiP).

2024 – 2026

Master of Laws (LL.M.), *KU Leuven*
Major International and European Law, minor Fiscal Law. **Cum laude.** Thesis: *Protecting the Union's Data: An Analysis of the Applicability of Personal Data Protection Standards to EU Institutional Data* (promotor Prof. E. Muir). Whether Regulation (EU) 2018/1725 can protect EU institutional data in US cloud services against foreign access under the CLOUD Act and FISA 702.

2021 – 2025

Bachelor of Laws (LL.B.), *KU Leuven*
Thesis in ICT law: *De territoriale gevolgen van het recht op gegevenswissing ("recht op vergetelheid") volgens artikel 17 AVG (GDPR): Wat is de territoriale reikwijdte van het Europees recht op schrapping van zoekresultaten?* (in Dutch).

2018 – 2021

Bachelor of Electronics-ICT, Cloud & Cybersecurity, *Thomas More, Geel*
Cum laude. Final-year internship and thesis at EY (Active Directory security).

2010 – 2017

Secondary education, Mechanics (vocational), *KTA Heist-op-den-Berg*
Self-taught in programming and IT security alongside.

CERTIFICATIONS

Certified Ethical Hacker (Practical)
EC-Council — 2020

IT Fundamentals for Cybersecurity
IBM Specialization — 2021

CyberOps Associate
Cisco Networking Academy course — 2021

Linux Essentials (LE-1)
Linux Professional Institute — 2019

OPEN SOURCE

Genergy Dashboard
Maintainer of an open-source Home Assistant energy dashboard (JavaScript)

PUBLICATION

Aug 2026

"Het EU-VS Data Privacy Framework doorstaat eerste juridische toets in Latombe/Commissie"

Knowledge Centre Data & Society (with CiTiP KU Leuven). Analysis (in Dutch) of the General Court's judgment in *Latombe v Commission* (T-553/23) and its consequences for EU-US data transfers.

EXPERIENCE

Aug 2020 – Sep 2022

Ethical Hacker, *Cyber Armed Security (remote)*

- Internal and external network, Wi-Fi and web application penetration tests for clients in several sectors, including well-known companies.
- Azure and AWS configuration reviews, and security audits against CIS benchmarks and ISO 27001.
- Findings reports for technical teams and management, with risk ratings and remediation advice.

2019 – 2022

Independent Security Researcher, *bug bounty & responsible disclosure*

- Discovered **CVE-2019-19699**, an authenticated remote code execution (root) zero-day in Centreon IT monitoring software ≤ 19.10.
- Acknowledged by the University of Cambridge CSIRT, the U.S. Department of Defense (via HackerOne) and Centreon; letter of recommendation from delaware after reporting a critical vulnerability.
- Hack The Box Guru rank (peak #2 in Belgium); Cyber Security Challenge Belgium finalist (14th).

Mar – May 2021

Intern Cyber Security Consultant, *EY Belgium, Diegem*

Research into the Active Directory attacks most used by threat actors (Kerberoasting, Golden/Silver Tickets, DCSync, Zerologon) and their detection and mitigation; 141-page thesis.