**LUCAS QUINTAO**

jobs@lucasquintao.it | lucasquintao.it | linkedin.com/in/lucasrogerquintao

# CYBER SECURITY SPECIALIST

HACK THE BOX
CERTIFIED CTF PLAYER
HACKTHEBOX
CPTS
CERTIFIED PENETRATION TESTING SPECIALIST
SECURITY
BLUE TEAM
HACK THE BOX
CERTIFIED PRO LAB

## SUMMARY

I am a **T2 SOC Analyst** with experience in monitoring, detecting, and responding to cyber threats in enterprise environments. My expertise spans incident management, threat hunting, and leveraging a variety of security tools to protect digital assets. In addition, I currently manage a **Cybersecurity Community** (0xH3xSec) of over **1,200 professionals**, fostering networking opportunities, knowledge sharing, and career development.

## PROFESSIONAL EXPERIENCE

**SOC Analyst T2** for **Accenture SpA** (contractor) (February 2024 - till now)

**Activities:**

1. **Security Incident Management**: Operated in a regulated financial environment, continuously reviewed and triaged security alerts using SIEM, EDR, Microsoft Defender, Azure, Proofpoint, and other tools. Coordinated and responded promptly to incidents to minimize impact and ensure regulatory compliance.
2. **Support to T1 Operators**: Provided guidance to Level 1 analysts, improving their ability to accurately identify, analyze, and resolve security incidents.
3. **Security Process Improvement**: Collaborated with cross-functional teams to define and implement security processes that optimized incident management, reduced response times, and aligned with industry best practices.
4. **Threat Hunting and Advanced Analysis**: Conducted threat hunting activities to identify potential threats not detected by standard security controls.
5. **Threat Intelligence Analyst:** Experienced in handling alerts from threat intelligence vendors, including CVE vulnerabilities, leaked account credentials, stolen bank account details, and other threats.

**Full-Stack Developer (freelancer)** for **Yesnet srl** (August 2023 - November 2023)

**Activities:**

1. **Project management:** Managed the project lifecycle, including setting and meeting deadlines, budgeting, client communication, testing, delivery, and post-production maintenance.
2. **Full-Stack Development:** Created the entire backend and frontend infrastructure for a web application designed to sell digital business cards. Technologies used were PHP, Javascript, MySQL

**System Administrator** for **TechCare srl** (April 2022 – October 2023)

**Activities:**

1. **Client support**: Provided technical support to clients, troubleshooting and resolving hardware and software issues in a timely manner.
2. **Maintenance of Clients Hardware Assets**: Managed and maintained the company's hardware assets, including regular updates, repairs, and replacements to ensure optimal performance.
3. **Maintenance of the Client Network**: Oversaw the maintenance and monitoring of the clients network infrastructure, ensuring network security, performance, and reliability.

# EDUCATION

**HackTheBox Academy - Penetration Tester Path** (July 2023 – May 2024)

I completed the Penetration Tester path at HackTheBox Academy, a practical training program focused on penetration testing skills. Key topics included:

- **Penetration Testing Methodologies**: Conducting structured tests, including reconnaissance, exploitation, and attack strategies.
- **System and Application Security**: Identifying and exploiting vulnerabilities in Windows, Linux, Active Directory environments, and web applications.
- **Advanced Techniques**: Chaining vulnerabilities, lateral movement, post-exploitation, and privilege escalation.
- **Reporting and Risk Communication**: Delivering professional-grade reports with clear remediation strategies.

The program included continuous assessments and culminated in a successful black-box penetration test on a simulated Active Directory network, solidifying my expertise in identifying and exploiting vulnerabilities while effectively communicating findings.

**I.T.I.S. Cerebotani Lonato del Garda – High School Diploma** (September 2016 – June 2021)

I completed my high school education in Computer Science, gaining foundational knowledge and practical skills in:

- **Programming**: Development of Web applications using PHP, Python and Javascript.
- **Networking**: Network design, configuration, and troubleshooting with Cisco Packet Tracer.

This education provided a solid base for further studies and a career in IT.

# CERTIFICATIONS

**Completed**:

- **Certified Penetration Testing Specialist** (CPTS), 2023-2024
- **Cyber Apocalypse CTF 2024** (Team ranked 364th globally out of 5,694 participants), 2024
- **Introduction to Dark Web Operations**, 2025

**In progress**:

- **B1 German**, Expected 2025-2026
- **Certified Defensive Security Analyst (CDSA)**, Expected 2025-2026

# SKILLS

**HARD SKILLS**

- **Penetration Testing**: Experience in identifying and testing web application vulnerabilities (OWASP 10), network security assessments, Active Directory testing for misconfigurations, and vulnerability assessment using manual and automated techniques.
- **Cybersecurity Monitoring & Response**: Experienced in threat monitoring and incident management with tools like **SIEM, EDR, Microsoft Defender, and correlation systems**. Skilled in mitigating threats, including on-call availability for rapid response.
- **Programming & Scripting**: Proficient in Python and PHP scripting for automation; working knowledge of web development (HTML, CSS, JavaScript, PHP, and MySQL).
- **Office365 Tools**: Competent in using Word, Excel, and other Office365 tools for data analysis and reporting.

**SOFT SKILLS**

- **Incident Analysis**: Proficient in identifying patterns and anomalies to investigate and respond to security threats effectively.
- **Team Collaboration**: Strong ability to work within a SOC environment, sharing insights and supporting team efforts to enhance security operations.
- **Technical Adaptability**: Quick to learn and implement new tools and techniques to address emerging cyber threats.
- **Effective Communication**: Skilled in documenting findings clearly for both technical and non-technical stakeholders and contributing to knowledge sharing within cybersecurity teams.

# LANGUAGES

**Italian**: Native

**English**: B2

**German**: A2

**Portuguese**: Second language, fluent