

# LEONARDO O. OI

*Security Information Analyst*

*leonardo.oliveoi.02@gmail.com | +55 (11) 94385-2302 | LinkedIn: leonardooliveoi | Github: leooliveoi*

## PROFESSIONAL SUMMARY

As a Senior Pentester and Cybersecurity Consultant with extensive experience in conducting penetration tests for high-profile international clients, I have demonstrated success in:

- Led 30+ penetration tests in compliance-driven environments (PCI-DSS), identified 400+ vulnerabilities, including critical flaws and misconfigurations.
- Provided direct support to stakeholders, offering actionable recommendations for vulnerability mitigation.
- Conducted security tests on web and mobile apps, including SAST, DAST, and SCA.
- Improved penetration testing processes by adopting frameworks like Scrum, MITRE, NIST, and OWASP SAMM, enhancing service quality and operational efficiency.
- Provided cyber security services such as consulting, penetration testing and vulnerability assessment directly or as a third party to international clients such as Veracode, Intersec Worldwide, financial companies in India and Saudi Arabia.

## PROFESSIONAL EXPERIENCE

### OISECURITY – SÃO PAULO, SP, BRASIL

#### **Owner & Cybersecurity Consultant (Self-Employed) - Remote**

*December 2024 – Current (6 months)*

I have officially opened my own cybersecurity consulting firm, focusing on providing valuable security solutions and helping startups, small and medium enterprises to evolve their security posture and maturity.

In general, I already helped small financial companies in Saudi Arabia, and small companies in Brazil in addition with collaboration with Intersec Worldwide in different PCI-DSS Assessments. This firm is composed only by me and does not have a name in the market yet.

Worked mainly with PCI-DSS Standard and SAMA (Saudi Arabia Monetary Authority) Compliance.

## **REDBELT SECURITY – BERRINI, SP, BRASIL**

### **Senior Penetration Testing Consultant - Hybrid**

*February 2025 – February 2025 (Less than 1 month)*

I worked with the Red Team sector to provide penetration testing and Red Team campaigns for different large Brazilian companies. Due to differences in work model preferences and company expectations, we mutually agreed to conclude our collaboration earlier than initially planned.

## **INTERSEC WORLDWIDE – NEWPORT BEACH, CA, USA**

### **Principal Cybersecurity Consultant (Contractor) - Remote**

*October 2024 – March 2025 (6 months)*

I worked as a contractor with Intersec Worldwide on a six-month PCI-DSS project, serving as a Principal Cybersecurity Consultant. In this role, I collaborated with stakeholders to achieve the following:

- I conducted comprehensive penetration testing on critical assets, including web applications, VPN portals, internal networks, and cloud infrastructure, identifying and prioritizing over 50 vulnerabilities, with an 85% mitigation rate achieved within the project timeline.
- Collaborating closely with development teams through briefings and technical interviews, I helped reduce the average remediation time from 30 to 15 days by fostering clear communication and efficient follow-up.
- Additionally, I managed and executed retesting of remediated issues, ensuring almost 100% compliance on all retested controls, which contributed directly to the successful PCI-DSS certification of the client.

## **CYBERNETIK CO. – BOCA RATON, FL, USA – REMOTE**

*(Hired through Old DBMX Negócios LTDA.)*

### **Senior Penetration Tester (International)**

*August 2023 – October 2024 (1 year and 2 months)*

I collaborated with penetration testing teams on over 30 international projects for major industry players. I conducted 20 intrusion tests in critical environments requiring compliance with standards such as PCI-DSS, identifying over 300 vulnerabilities, including misconfigurations and critical issues.

Worked directly with stakeholders to assess risks and provide practical, effective recommendations to mitigate identified vulnerabilities, delivering efficient, high-quality post-test support.

Managed operational processes before, during, and after tests, including Platform Onboarding, Kick-Off Calls, Recurring Updates, Briefing, and Troubleshooting.

Familiar with tools and frameworks for auditing complex systems, including:

- Web Applications: APIs, IVRs, portals, and critical interfaces.
- Mobile Applications: Android and iOS.
- Critical Internal and External Networks.
- Cloud Environments: AWS and Azure.

I conducted security tests on robust and mobile applications, including:

- SAST (Static Application Security Testing)
- DAST (Dynamic Application Security Testing)
- SCA (Software Composition Analysis)

By adopting methodologies such as Scrum, MITRE, NIST, and OWASP SAMM, I improved internal processes for executing and managing pentests, enhancing service quality, reliability, and excellence.

### **Penetration Tester (International)**

*August 2022 – August 2023 (1 year)*

I participated in more than 10 international offensive security audits, where I was able to communicate with around 6 project stakeholders (Developer, Project Manager, Security Teams, among others), and to found around 10 to 30 security flaws per project, using high-level methodologies.

Used the BurpSuite Pro tool to perform manual approaches in Web applications and APIs, where I found the main flaws such as SQL Injection, Improper & Broken Access Control, Cross-Site Scripting, user enumeration, among others.

Familiar with automated analysis tools such as Nessus, OpenVAS, and Nikto, which allowed me to have a broader view of the current security structure and maturity of the applications in a short space of time.

Performed more than 50 port and service scans with NMAP and NetCat, discovering hidden vulnerabilities in unprotected or outdated services.

I used the MobSF (Mobile Security Framework), SonarQube, Jadx and FRIDA tools to perform SAST, DAST and SCA on mobile applications, increasing the testing speed on Android and iOS applications by 20%.

### **Intern Information Security Analyst**

*September 2021 – August 2022 (1 year and 1 month)*

Assisted the senior cybersecurity team with penetration testing activities across various environments, including web and mobile applications, in addition to network infrastructures.

Conducted vulnerability scanning using industry-standard tools like Kali Linux and Burp Suite under the supervision of senior analysts.

Participated in the preparation of Information Security Reports, including documentation of vulnerabilities, risk ratings, and recommendations for remediation.

Collaborated on security incident investigations, helping to identify the root causes and assist in drafting incident response reports.

Supported the team with security monitoring tasks using SIEM, IDS/IPS, and other monitoring tools to track and respond to security threats in real-time.

Developed basic scripts in Python and Bash to automate repetitive tasks, improving the efficiency of vulnerability testing and system monitoring processes.

Participated in team meetings and client calls, gaining exposure to client-facing activities and learning to communicate complex security issues in a clear, actionable manner.

In addition, I completed more than 4 specialized training courses in information security at large companies such as CISCO, INE, Solyd Offensive Security and (ISC)2. During this period, I obtained the SYCP certification, which gave me more visibility

within the company and helped me develop skills that allowed me to work as a Pentester in 3 international projects.

## **EDUCATION**

### **FACULDADE DESCOMPLICA, SÃO PAULO, BRASIL**

#### **MBA in Innovation Management and Entrepreneurship (MEC-Accredited)**

*January 2025 – Current (Completion January 2026)*

Training focused on strategic tools and market-driven approaches to foster innovation and business development in digital environments.

Skilled in applying innovation management, entrepreneurship, data analysis, marketing strategy, and growth hacking to solve real-world business problems.

Specialized in understanding consumer behavior and network dynamics to create and scale impactful solutions across industries.

Developed both technical and behavioral skills through a hands-on, innovation-driven methodology, enabling immediate application in professional settings.

Integrated cybersecurity considerations into innovation strategies by exploring how digital trust, data protection, and secure product development enhance the resilience and competitiveness of modern businesses. Applied a security-by-design mindset in entrepreneurial contexts to ensure scalable and secure digital growth.

#### **MBA in Information Security (MEC-Accredited)**

*June 2023 - July 2024 (1 year)*

Training in Information Security with a focus on the application of technological resources and procedures to ensure the reliability, integrity, and availability of corporate data.

Skilled in implementing security measures that prevent invasions into corporate networks, both local and remote.

Specialized in structuring policies and practices for managing technological resources, ensuring solid and effective corporate governance through information security strategies.

Familiar with the regulatory environment and the legal aspects of information security, using them as resources to enhance corporate governance.

## **CISCO NETWORKING ACADEMY, BRASIL, ONLINE**

### **CyberOps & CCNA Bootcamp**

*December 2021 - April 2022 (5 months)*

Solid foundation in TCP/IP, OSI model, routing protocols, VLANs, and subnetting.

Skilled in configuring Cisco devices, implementing firewalls, IPS, ACLs, and securing enterprise networks.

Hands-on experience with SOC operations, SIEM tools, incident triage, and response frameworks such as NIST.

Familiar with network automation using REST APIs, Ansible, and SNMP to enhance security and operational efficiency.

## **UNIVERSIDADE ANHEMBI MORUMBI, SÃO PAULO, BRASIL**

### **Bachelor's degree in system Analysis and Development (MEC-Accredited)**

*January 2020 - July 2022*

Training focused on operating systems, software development, cloud computing, system analysis, and IT project management.

Developed foundational skills in designing, implementing, and managing technological solutions, with practical knowledge applicable to cybersecurity and secure software development.

## **LANGUAGES**

Brazilian Portuguese (Fluent)

English (Fluent)

## **CERTIFICATIONS**

- Certified in Cybersecurity (CC).
- SYCP (Solyd Certified Pentester).

- eJPT (eLearnSecurity Junior Penetration Tester).
- CAPC (Cybersecurity Awareness Professional Certified).
- ISO 27k Associate.
- Lei Geral de Proteção de Dados (LGPD).

## **SKILLS**

- Penetration Testing: Web, Mobile, Network, Cloud
- Compliance: PCI-DSS, ISO 27001, GDPR, LGPD
- Vulnerability Assessment & Remediation.
- Security Monitoring: SIEM, XDR, IDS/IPS.
- Incident Response & Forensics.
- Scripting: Python, Bash, PowerShell
- Report Writing & Client Communication.
- Governance, Risk, and Compliance (GRC).

## **TOOLS & TECHNOLOGIES**

- Tools: Kali Linux, Burp Suite, Nessus, etc
- Operational Systems: Ubuntu, Debian, Fedora, Windows.
- Docker, Podman, Distrobox, WSL1, WSL2.
- Cloud Security Platforms (AWS, Azure).
- Active Directory (AD) Assessment.
- Firewalls, VPN, Security Policies & Procedures.
- SAST, SDA, and DAST (MobSF, SonarQube, etc.).
- Vulnerability Scoring (PCI-DSS, CVSSv3).
- Cloudflare Management.
- PFSense, FledDM, Wazuh, Elastic Search, Kibana.
- Logstash, FileBeat, Frida Tool.
- OpenVPN, Tailscale, Microsoft Azure Management.

## **PROFESSIONAL MEMBERSHIPS**

### **INSTITUTO DE DEFESA CIBERNÉTICA**

#### **Member of the Public Committee**

*July 2025 – Jan 2025*

### **(ISC)<sup>2</sup> MEMBERSHIP**

#### **Associated Member**

*Jan 2024 – Jan 2025*

## **COURSES AND CERTIFICATES**

### **(ISC)<sup>2</sup> - Pearson VUE**

- Certified in Cybersecurity (CC) Self-Paced – October 2022

### **TCM Security Academy**

- Linux Privilege Escalation for Beginners – January 2024
- Windows Privilege Escalation for Beginners – January 2024
- Practical Web Application and Testing – May 2023
- Movement Pivoting and Persistence – January 2023
- Mobile Application Penetration Testing – December 2022
- Practical Ethical Hacking – November 2022

### **Cisco Academy**

- CyberOps Associate – April 2022
- CCNA: Introduction to Networks – February 2022
- Cybersecurity Essentials – October 2021

### **INE Security – eLearnSecurity**

- Junior Penetration Tester Learning Path – January 2022
- Profession Penetration Tester Learning Path – May 2022

### **Solyd Offensive Security**

- Professional Penetration Tester v2021 – January 2022

### **Certiprof**

- Cybersecurity Awareness Professional Training – August 2024
- Lei Geral de Proteção de Dados (LGPD) – April 2022

### **Faculdade Descomplica**

- Cyber Operations – September 2023
- Cyber Threat Management – August 2023
- Network Defense – August 2023
- Endpoint Security – July 2023
- Cybersecurity Essentials – June 2023
- Network Essentials – June 2023

### **Amazon Web Services Academy - AWS**

- AWS Academy Cloud Foundations – May 2022



### **The Cloud Bootcamp**

- Intensive Multicloud, DevOps and AI – Oct 2024

### **IBSEC – Brazilian Institute of Cybersecurity**

- Fundamentals of Cybersecurity – April 2022

### **Udemy**

- Hacking for Beginners – March 2024
- Professional Ethical Hacking – March 2022

### **Cybersecurity and Infrastructure Security Agency (CISA)**

- 210-06 ICS Cybersecurity Threats – July 2024

### **SkillFront**

- ISO|IEC 27001 Information Security Associate – May 2023
- Foundations of Business and Entrepreneurship – May 2023