

# CRISTIAN SOUZA

✉ cristianmsbr@gmail.com | 🌐 cristian.sh | 🔗 cristianzsh | in cristianzsh | 📧 cristianzsh | 🎓 Cristian Souza | Lattes CV

## SUMMARY

I am a cyber security professional based in Brazil with extensive experience in information security, system administration, computer vision, and image processing. Since high school, I have worked on research projects in various areas, including information security, privacy, malware analysis, software-defined networking, and artificial intelligence.

In addition to my work, I am currently pursuing a PhD degree in Computer Science. I believe that the combination of my practical experience and academic study allows me to have a broad and innovative perspective on the cyber security challenges faced by companies today.

I enjoy experimenting with new tools and technologies and, whenever possible, developing new open-source projects to help the community. My main research interests include malware analysis, operating systems, and artificial intelligence.

## EDUCATION

<b>University of São Paulo (USP)</b> <i>Ph.D. in Computer Science</i>	São Paulo, Brazil 2024 – Present
<b>Centro Paula Souza (CPS/FATEC-SP)</b> <i>Master's Degree in Management and Technology</i>	São Paulo, Brazil 2023 – 2024
<b>Instituto Daryus de Ensino Superior Paulista (IDESP)</b> <i>Postgraduate Degree in Digital Forensics and Cyber Investigation</i>	Remote 2022 – 2023
<b>Centro de Inovação VincIT (UNICIV)</b> <i>Postgraduate Degree in Ethical Hacking and Cyber Security</i>	Remote 2022 – 2022
<b>Federal Institute of Rio Grande do Norte (IFRN)</b> <i>Bachelor of Technology (BTech) in Computer Systems Networking</i>	Natal, Brazil 2019 – 2022
<b>Digital Metropolis Institute (IMD)</b> <i>Certificate Program in Electronics</i>	Natal, Brazil 2018 – 2019
<b>Federal Institute of Rio Grande do Norte (IFRN)</b> <i>Certificate Program in Informatics</i>	Natal, Brazil 2015 – 2018

## EXPERIENCE

<b>Kaspersky Lab</b> <i>Digital Forensics and Incident Response Specialist</i>	Remote, Brazil Dec. 2023 – Present
<b>Daryus Consultoria e Treinamento</b> <i>Cyber Security Consultant &amp; Professor</i>	Remote, Brazil Jan. 2021 – Dec. 2023
<ul style="list-style-type: none"><li>• Conducted penetration testing in web applications, infrastructures, and mobile applications.</li><li>• Performed reverse engineering of PE and APK files.</li><li>• Conducted computer forensics investigations.</li><li>• Conducted cloud computing audits to ensure security best practices were followed.</li><li>• Provided guidance on secure development practices.</li><li>• Led red team exercises to identify vulnerabilities in organizations' security defenses.</li></ul>	

- Designed and executed phishing campaigns to raise awareness and test employees' security awareness.
- Led the creation and implementation of robust incident response playbooks, optimizing response strategies for swift and effective resolution.
- Actively contributed to ISO 27001 audits, ensuring adherence to information security standards.
- Conducted audits of critical systems to ensure they meet security standards.
- As a professor of post-graduate courses, instructed students in various topics related to information security, including: Malware analysis and reverse engineering; Mobile and wireless penetration testing; Incident response; Windows & Linux security; Secure programming; Network security; and IoT security.
- Instructed courses in web application security, secure programming, and ethical hacking, with a focus on the following topics: OWASP Top 10 and Secure Coding Practices; OWASP Proactive Controls and API Security; SAST, DAST, and SCA techniques; DevOps and DevSecOps methodologies; Threat modeling for software security; Network, web application, and wireless network penetration testing.
- Additionally, taught other related courses, such as Penetration Testing, Open-source Intelligence (OSINT), Ethical Hacking Foundation, Secure Programming Foundation, and NIST Cyber Security Framework.

## **Federal Institute of Rio Grande do Norte (IFRN)**

*Researcher, R&D Software Developer & Tutor*

Natal, Brazil

*Apr. 2016 – Jun. 2022*

- Conducted research in information security, focusing on malware analysis and detection, software-defined networks, and moving target defense.
- Authored and published research papers in multiple conferences and journals to share findings and contribute to advancements in the fields.
- Conducted research in computer vision and image processing and developed practical applications in the field.
- Designed and developed an ALPR (Automatic License Plate Recognition) application for embedded hardware, with a patent application filed.
- Developed an OCR (Optical Character Recognition) application to extract text from images.
- Created a deep learning-based face recognition application and API.
- Main programming languages: Java and Python.
- Other technologies: OpenCV, dlib, REST, Flask, MySQL, RFID.
- Provided support to students studying operating systems, offering guidance and assistance with course materials.
- Provided assistance to students studying algorithms and data structures, offering guidance and support with course materials.

## **SutHub**

*Back-end Developer*

Remote, Brazil

*Nov. 2020 – Apr. 2021*

- Designed and developed multiple Robotic Process Automation (RPA) tools to automate repetitive tasks and improve productivity.
- Conducted Static Application Security Testing (SAST) in the core system to identify and mitigate potential security risks.
- Main programming language: Python.
- Other technologies: Selenium, AWS (EC2, CloudWatch, and S3), MySQL.

## **Actions Security**

*Information Security Analyst*

Remote, Brazil

*May 2018 – Jul. 2019*

- Helped develop a Web Application Firewall (WAF).
- Utilized Elastic Stack, Docker containers, and reverse proxies to achieve project goals.
- Successfully implemented an OpenStack infrastructure, enabling increased efficiency and scalability.
- Conducted penetration tests in web applications to identify security vulnerabilities.
- Main programming languages: Python and C.
- Other tools and technologies: OWASP Top 10, AWS, OpenStack, ModSecurity, Linux.

## SKILLS

---

**Languages:** Portuguese (native), English (advanced level), Spanish (basic level)

**Programming:** C, Java, Python, Shell Script, YARA, SQL

**Generic:** Penetration Testing, Computer Forensics, Malware Analysis, Reverse Engineering, FTK, OWASP Top 10, Linux Administration, AWS, Git, Docker, Elastic Stack, Flask, REST

## CERTIFICATIONS

---

**Certified Information Systems Security Professional (CISSP)**, (ISC)<sup>2</sup>

**GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)**, SANS Institute

**GIAC Reverse Engineering Malware (GREM)**, SANS Institute

**GIAC Experienced Forensic Analyst (GX-FA)**, SANS Institute

**GIAC Certified Forensic Analyst (GCFA)**, SANS Institute

**GIAC Response and Industrial Defense (GRID)**, SANS Institute

**GIAC Certified Incident Handler (GCIH)**, SANS Institute

**GIAC Cyber Threat Intelligence (GCTI)**, SANS Institute

**CompTIA Advanced Security Practitioner (CASP+)**, CompTIA

**ISO/IEC 27001 Lead Auditor**, PECB

**Computer Hacking Forensic Investigator (CHFI)**, EC-Council

**Certified Ethical Hacker (Practical)**, EC-Council

**Certified Ethical Hacker (CEH)**, EC-Council

**Pentest+**, CompTIA

**BSD Specialist**, Linux Professional Institute

**LPIC-3: Security**, Linux Professional Institute

**LPIC-2: Linux Engineer**, Linux Professional Institute

**LPIC-1: Linux Administrator**, Linux Professional Institute

**Linux+**, CompTIA

**Certified in Cybersecurity**, (ISC)<sup>2</sup>

## HONORS & AWARDS

---

<b>Best Paper Award, XXV SBSeg</b> <i>Brazilian Computer Society</i>	2025
---	------

<b>Youth Digital Ambassador</b> <i>Global Digital Forum</i>	2025
--	------

<b>Top-3 Nominees</b> <i>Global Digital Forum</i>	2025
--	------

<b>Outstanding Reviewer Award, XLIII SBRC</b> <i>Brazilian Computer Society</i>	2025
--	------

<b>GIAC Advisory Board</b> <i>Global Information Assurance Certification (GIAC)</i>	2024
--	------

<b>CEH Master</b> <i>EC-Council</i>	2023
<b>Academic Honors Diploma (Summa Cum Laude)</b> <i>Federal Institute of Rio Grande do Norte</i>	2022
<b>Distinguished Paper Award, XL SBRC</b> <i>Brazilian Computer Society</i>	2022
<b>Capture the Flag Champion</b> <i>Darkwaves Conference</i>	2018

## RESEARCH PAPERS

---

### Journal articles

- SDN-based Solutions for Malware Analysis and Detection: State-of-the-art, Open Issues and Research Challenges  
Journal of Information Security and Applications - Elsevier, 2025  
DOI: 10.1016/j.jisa.2025.104145
- A hybrid approach for malware detection in SDN-enabled IoT scenarios  
Internet Technology Letters - Wiley, 2024  
DOI: 10.1002/itl2.534
- Securing Software-Defined Networks Through Adaptive Moving Target Defense Capabilities  
Journal of Network and Systems Management - Springer Nature, 2023  
DOI: 10.1007/s10922-023-09746-z
- On detecting and mitigating phishing attacks through featureless machine learning techniques  
Internet Technologies Letters - Wiley, 2020  
DOI: 10.1002/itl2.135

### Book chapters

- Embedded System for Access Control Based on Facial Biometry and RFID  
Advances in Intelligent Systems and Computing - Springer Nature, 2018  
DOI: 10.1007/978-3-030-02683-7\_62

### Conference proceedings

- Foremost-NG: An Open-Source Toolkit for Advanced File Carving and Analysis  
XXV Brazilian Symposium on Cybersecurity (SBSeg), 2025  
DOI: 10.5753/sbseg\_estendido.2025.12307
- Lessons Learned from the ShrinkLocker Ransomware: From Response to Detection  
XXV Brazilian Symposium on Cybersecurity (SBSeg), 2025  
DOI: 10.5753/sbseg\_estendido.2025.11387
- On the Use of Machine Learning for Modern IoT ELF Malware Detection  
IEEE Latin American Conference on Computational Intelligence, 2025  
*To be published*
- Avaliação de algoritmos de machine learning para detecção de malware IoT no dataset IoT-23  
XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), 2024  
DOI: 10.5753/sbseg.2024.241472
- Detecção de malware em ambientes IoT habilitados por SDN  
XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2024  
DOI: 10.5753/wpeif.2024.2594

- An Adaptive Moving Target Defense Approach to Software-Defined Networking Protection  
36th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2023  
DOI: 10.1109/NOMS56928.2023.10154278
- Abordagem Adaptativa para Proteção de Redes SDN Utilizando Moving Target Defense  
XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2022  
DOI: 10.5753/sbrc.2022.222378
- Freki: Uma Ferramenta para Análise Automatizada de Malware  
XXI Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg), 2021  
DOI: 10.5753/sbseg\_estendido.2021.17340
- MTD para Proteção de Redes SDN  
X Conferência Nacional em Comunicações, Redes e Segurança da Informação (ENCOM), 2020
- PhishKiller: Uma Ferramenta para Detecção e Mitigação de Ataques de Phishing Através de Técnicas de Deep Learning  
XIX Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg), 2019  
DOI: 10.5753/sbseg\_estendido.2019.14009

### Threat research and reports

- Forensic journey: hunting evil within AmCache  
Securelist – Kaspersky Lab, 2025
- Driver of destruction: How a legitimate driver is being used to take down AV processes  
Securelist – Kaspersky Lab, 2025
- Outlaw cybergang attacking targets worldwide  
Securelist – Kaspersky Lab, 2025
- Incident response analyst report 2024  
Global Emergency Response Team (GERT) – Kaspersky Lab, 2025
- Attackers exploiting a patched FortiClient EMS vulnerability in the wild  
Securelist – Kaspersky Lab, 2024
- Analysis of Elpaco: a Mimic variant  
Securelist – Kaspersky Lab, 2024
- Ymir: new stealthy ransomware in the wild  
Securelist – Kaspersky Lab, 2024
- ShrinkLocker: Turning BitLocker into ransomware  
Securelist – Kaspersky Lab, 2024
- Incident response analyst report 2023  
Global Emergency Response Team (GERT) – Kaspersky Lab, 2024
- Using the LockBit builder to generate targeted ransomware  
Securelist – Kaspersky Lab, 2024

## VULNERABILITY DISCLOSURES

<b>CVE-2025-7771</b>	2025
<i>Code Execution, Base score: 8.7 HIGH, Vector: CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H</i>	
<b>CVE-2019-7634</b>	2019
<i>Cross-site Scripting (XSS), Base score: 5.4 MEDIUM, Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N</i>	

## OPEN-SOURCE PROJECTS

---

### **Freki**

*Malware analysis platform*

*Python*

- Features: static analysis, user management, REST API, and Web UI.

### **forensictools**

*Collection of forensic tools*

*Inno Setup*

- Toolkit designed for digital forensics, offering a wide array of tools.

### **OpenBSD self-hosted**

*Deploy private services on top of OpenBSD*

*Shell Script*

- Features: automatically installs and configures cloud, git, and email services.

### **AmCache-EvilHunter**

*Identify suspicious files in Amcache.hve*

*Python*

- Features: identify suspicious executables, filter records, VirusTotal integration.

### **k-evtrace**

*Applies custom Sigma rules to Kaspersky EVTX logs*

*Python*

- Features: Sigma rule parsing, IOC extraction, OpenTIP integration.

### **Foremost-NG**

*Data carving tool*

*C*

- Features: recover files based on headers and footers, VirusTotal lookup.

### **Segurança em servidores Linux**

*Mini e-book about Linux security*

*Markdown*

- Written in Portuguese, it encompasses security practices for Linux systems and services.

### **JCEditor**

*Advanced text editor*

*Java*

- Features: syntax-highlighting, cross-platform, Swing UI.

## PATENTS & SOFTWARE

---

### **BR 10 2018 015493 1**

2018

*Sistema Embarcado para Reconhecimento Automático de Placas de Veículos*

### **BR512024001975-8**

2024

*Heimdall-NG - Interface administrativa*

### **BR512024000157-3**

2024

*Heimdall: Solução para detecção de artefatos maliciosos em ambientes IoT por meio de machine learning*

### **BR512022002010-6**

2022

*PhishKiller*

### **BR512019000143-5**

2019

*NAVI RPi Face Recognition*

### **BR512019000144-3**

2019

*NAVI-ALPR*

<b>BR512019000141-9</b> <i>NAVI Face Recognition API</i>	2019
<b>BR512019000140-0</b> <i>Sistema Embarcado para Medição de Pluviosidade e Gerenciamento SNMP</i>	2019
<b>BR512018000086-0</b> <i>OCR-NAVI</i>	2018

## ACADEMIC SERVICE

---

- Internet of Things, Elsevier** - Reviewer
- Computer Communications, Elsevier** - Reviewer
- International Journal of Cognitive Computing in Engineering (IJCCE), Elsevier** - Reviewer
- XXV Brazilian Symposium on Cybersecurity (SBSeg 2025)** - Reviewer
- XLIII Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2025)** - Reviewer

## VOLUNTEERING

---

- OWASP Foundation** Natal, Brazil  
*Chapter Leader* Dec. 2022 – Present
  - As chapter leader, my responsibilities include efficiently maintaining the chapter, organizing engaging information security meetings, and conducting workshops.
- Federal Institute of Rio Grande do Norte** Natal, Brazil  
*Android Developer* Sep. 2015 - Feb. 2016
  - Volunteered to develop a mobile app for monitoring water usage at IFRN (campus Natal Central).