**Leonardo Uzcategui MsC, eJPT, CC**

Orlando, FL | 551.327.5624 |uzcategui@gmail.com | https://www.linkedin.com/in/leonuz/

Propose and implement significant security enhancements for the organization. In addition to auditing, advising, supporting, informing, and providing training and awareness in network and information security.

**CORE COMPETENCIES**

|  |  |  |
| --- | --- | --- |
| **Security Policies** | **Network Administrator** | **Penetration Testing** |
| **Security Awareness and Education** | **Incident Detection and Response** | **Governance, Risk and Compliance** |
| **Vulnerability Scan** | **SOC Analyst** | **System Administrator** |

**PROFESSIONAL EXPERIENCE**

**CA2 Security - Orlando, FL**

***Chief Technology Officer (CTO) 2022 – present***

At CA2 Security we lean on business and risk management principles, creativity, agility, and trusted partnerships to help our clients reduce cyber risk through Continuous, Adaptable, and Actionable cybersecurity programs.

* Develop technical aspects of the company’s strategy to ensure alignment with its business goals
* Discover and implement new technologies that yield competitive advantage
* Help departments use technology profitably
* Supervise system infrastructure to ensure functionality and efficiency
* Build quality assurance and data protection processes
* Monitor KPIs and IT budgets to assess technological performance
* Use stakeholders’ feedback to inform necessary improvements and adjustments to technology
* Communicate technology strategy to partners and investors
* Working with Infosec frameworks such as MITRE, NIST, ISO

**IDTIC, C.A. – Merida, Venezuela**

***Security Consultant 2005 – 2021***

Work with multiple clients to evaluate existing IT procedures, conduct penetration tests, vulnerability assessment, risk management, security policies and discuss problems and solutions with managers and staff.

* Maximize efficiency in protecting client data and information systems, networks, and software.
* Work closely with clients IT departments to correct network security problems.
* Work with managers, engineers, and other security analysts to decrease risks for an organization.
* Supervise and guide security teams of managers, engineers, and other technical or security employees.
* Plan and design security architectures for IT projects.
* Research cybersecurity criteria, security systems, and validation procedures.
* Probe and provide security solutions referencing business-standard analysis criteria.
* Update and upgrade security systems as needed.
* Deliver official reports that summarize test findings.
* Oversee and conduct tests for system vulnerabilities.
  + Perform penetration tests on computer systems, networks and applications
  + Create new testing methods to identify vulnerabilities
  + Perform physical security assessments of systems, servers and other network devices to identify areas that require physical protection
  + Pinpoint methods and entry points that attackers may use to exploit vulnerabilities or weaknesses
  + Search for weaknesses in common software, web applications and proprietary systems
  + Research, evaluate, document and discuss findings with IT teams and management
  + Review and provide feedback for information security fixes
  + Establish improvements for existing security services, including hardware, software, policies and procedures
  + Identify areas where improvement is needed in security education and awareness for users
  + Be sensitive to corporate considerations when performing testing (i.e. minimize downtime and loss of employee productivity)
  + Stay updated on the latest malware and security threats

**RedULA – Merida, Venezuela**

***Cybersecurity Specialist 2001 – 2005***

*Responsible for the coordination of the Network and security monitoring group for the WAN, LAN and Wireless links within the University of Los Andes. Founding Member of the Computer Security Group of the Universidad de los Andes.*

* Design the security capabilities for the entire university
* Implement firewall policies based in Cisco PIX 535 hardware
* Discovering vulnerabilities and risks in networks, software systems and University data centers with ongoing vulnerability scans
* Monitoring all network data and ensuring hardware and software applications are updated.
* Implementation of safety policies under the BS-7799 standard.

**EDUCATION, CREDENTIALS & TRAINING**

**MsC. Telecommunication,** University of Los Andes (ULA), Mérida, Venezuela.

**BS. Electrical Engineering,** University of Los Andes (ULA), Mérida, Venezuela.

**ISC2-CC** - Certified in Cybersecurity

**eJPT** - Junior Penetration Tester

**BS 7799-2 -** Lead Auditor (expired)

**CCNA** - Cisco Certified Network Associates (expired)

**LPIC-1** - Linux Professional Institute (expired)

**eCCPTv2** - Certified Professional Penetration Tester (Schedule to March/2023)

**ISCP-CISSP** - Certified Information Systems Security Professional (Planned to Q4 2023)

**Completed Courses Include:**

|  |  |
| --- | --- |
| Practical Malware Analysis & Triage | SOC Analyst |
| Practical Web Application Security and Testing | Autopsy Forensic Tool Training |
| AWS Cloud Practitioner Essentials (Second Edition) | Microsoft Azure fundamentals |
| CISSP Preview |  |
| Scrum Foundation Professional Certificate |  |
| ICSI Certified Network Security Specialist |  |

<https://leonuz.github.io>

<https://github.com/leonuz>

<https://leonuz.medium.com>

**COMMUNITY ENGAGEMENT**

* From 2001 to 2013 I participated as an pro-bono instructor/teacher in Network Security and Wireless Technologies workshops for the Escuela Latino Americana de redes (EsLaRed). Gaining extensive knowledge about the methods of information transmission (training tools, awareness mechanisms, etc.). EsLaRed received the 10th annual Jonathan B. Postel service award for promoting the Internet in Latin America. ([more info](https://www.internetsociety.org/news/press-releases/2008/leading-latin-american-foundation-eslared-receives-10th-annual-jonathan-b-postel-service-award-promoting-internet-latin-america/))
* Development an open source, low cost, low electricity consumption and portable, communication center, that is easy to deploy, design to be used in disaster and / or high risk areas. RADCOM (Radio Comunicaciones Móviles/ Radio Mobile Communications). This project was financed by the FRIDA Program, in the 2009 year, an initiative of LACNIC “Registry of Internet addresses for Latin America and the Caribbean”
* Development of a GNU / Linux distribution that integrates a VoIP Telephone System and a Terminal Server for the management of Telecommunications Centers called [Colibrí-IP](http://web.archive.org/web/20071012052511/http:/idtic.org/index.html)

It was financed in part by the “Institute for the connectivity of the Americas, ICA” , through the [TRICALCAR program](https://www.eslared.net/sites/default/files/2020-07/presentacion_proyecto_TRICALCAR.pdf) (Weaving Wireless Networks in Latin America and the Caribbean) in the year 2007

* Researcher classified type “A” in the Program to Stimulate Innovation and Research (PEII) of the National Observatory of Science, Technology and Innovation (ONCTI) of the Ministry of Popular Power for Science and Technology of the Bolivarian Republic of Venezuela in the 2011 call