

LEANDRO PAREJA

Lexington Park, 20653 | (561) 445-7536 | lee.pareja1@outlook.com | LinkedIn | U.S. Citizen

<https://www.linkedin.com/in/leandro-pareja-2b4377382/>

CompTIA SecurityX (CASP+) certified cybersecurity professional with hands-on systems administration experience across production servers and multiple nodes supporting 20,000+ active users. Clearance eligible with no active clearance. Skilled in identity and access management, server monitoring, network traffic analysis, authentication testing, vulnerability research, API integration, and technical documentation. Committed to learning and eager to contribute reliable infrastructure operations and analytical skills to defense contracting and federal IT.

CERTIFICATIONS

Cisco Certified Network Associate (CCNA) | IN PROGRESS

Microsoft Certified: Azure Administrator Associate (AZ-104) | IN PROGRESS

CompTIA SecurityX (formerly CASP+) Certification | Earned September 2026

LinkedIn Windows 11: Configure and Support Core Services Certification | Earned September 2026

LinkedIn Windows 11: Administration Certification | Earned September 2026

Global Career Accelerator Data Analysis Certification | Earned July 2026

Global Career Accelerator Data Visualization Certification | Earned July 2026

Global Career Accelerator Intercultural Skills Certification | Earned July 2026

Global Career Accelerator AI Professional Skills Certification | Earned July 2026

EXPERIENCE

Legioner Solutions

Founder | Systems Administration and Application Security

Hours per week: Approx. 35–40 | Series/Grade: N/A (private sector)

Boca Raton, FL

October 2023 – August 2025

- Performed systems administration across production servers and multiple nodes supporting 20,000+ active users; managed server configurations, application deployments, maintenance, and technical troubleshooting.
- Engineered API integrations and real-time data pipelines using MongoDB, JSON, and the Google Sheets API; managed server logs and user requests, resolved data integrity issues, and maintained technical documentation.
- Automated Identity and Access Management (IAM) and role-based access control (RBAC) workflows, reducing administrative overhead by 70% while improving user verification and account administration.
- Led a distributed team of contributors, established technical priorities, and coordinated feature development, bug fixes, and release schedules across time zones.
- Monitored servers and multiple nodes through log review, error tracking, and availability checks; maintained 99.9% uptime by investigating service disruptions, resolving faults, and restoring reliable operations.
- Developed React dashboards deployed through Railway and Vercel to centralize server activity and operational data, enabling nontechnical stakeholders to monitor production environments and player engagement.
- Integrated Epic Online Services (EOS) and Steam APIs for authenticated server and player data; assessed undocumented authentication behavior through controlled testing and documented observed security risks.
- Managed a \$300 monthly infrastructure budget and maintained regular communication with users and contributors to address technical needs and support reliable service delivery.

TECHNICAL PROJECTS

Application Security & Network Traffic Assessment

Personal Project

Self-Directed

2025

- Conducted black-box analysis of client-server communications; analyzed outbound network traffic, DNS behavior, telemetry, and host-level traffic controls to assess application behavior and authentication risks.
- Assessed EOS and Steam authentication workflows using public documentation, controlled testing, and direct observation to identify weaknesses in identity verification and third-party service interactions.
- Discovered and documented an authentication-related information exposure vulnerability involving player and server data in EOS/Steam workflows; responsibly disclosed the findings to Studio Wildcard.

Unreal Engine 5 Security Assessment & Responsible Disclosure

Personal Project

Self-Directed

2025

- Developed a custom Unreal Engine 5 mod using Blueprint scripting; examined client-side architecture and command execution behavior to support application security testing and vulnerability assessment.
- Identified and documented an access control bypass that allowed unauthenticated users to load unapproved mods onto official multiplayer servers, circumventing restrictions on unauthorized content.
- Responsibly disclosed the vulnerability to Studio Wildcard, documenting the observed behavior and potential security impact to support remediation and reduce the risk of unauthorized server content.

EDUCATION

Florida Atlantic University

Bachelor of Science in Data Science and Analytics

Boca Raton, FL

Expected Spring 2027

- GPA: 3.80 / 4.00
- Honors: Dean's List (Spring 2026)
- Relevant Coursework: Advanced Business Analytics, Data Mining & Predictive Analytics, Data Management & Analysis with Excel, Introduction to Business Analytics & Big Data, Tools for Data Science, Mathematics of Data Science

Palm Beach State College

Associate in Science in Computer Programming

Boca Raton, FL

December 2024

- GPA: 3.50 / 4.00
- Relevant Coursework: Introduction to Programming, C# Programming, Systems Analysis and Design, Network Technologies, Information Technology

TECHNICAL SKILLS

Security & Access Control: Vulnerability assessment, IAM, RBAC, authentication testing, responsible disclosure

Programming & Automation: Python, JavaScript, Node.js, SQL, R, C#, React, Tailwind, MongoDB

Operating Systems & Infrastructure: Windows 11, VMware, Docker, Railway, Vercel, Git/GitHub

Network Security & Operations: Systems administration, server and node monitoring, log analysis, troubleshooting, network traffic analysis, DNS, host-level traffic controls, CI/CD basics

Data, Documentation & Collaboration: ETL pipelines, API integration, database design, Excel, Microsoft Office, Teams, Google Sheets, technical documentation, leadership | Remote availability

LANGUAGES

English (Native) | Spanish (Fluent)