Leandro Federico Juárez

Splunk Consultant & Architect · SIEM Engineer · Certified Splunk Instructor

Argentina (Remote) | linkedin.com/in/leandrofjuarez | English: Full Professional Proficiency | Spanish: Native

PROFILE

Splunk Enterprise Certified Architect and Core Certified Consultant with 12+ years in IT and 5+ years specialized in Splunk—and one of a small group of professionals also accredited as an official Splunk Certified Instructor, combining deep architecture expertise with proven, current mastery of the platform. Deep hands-on expertise in distributed and clustered deployments (Indexer & Search Head Clustering), data onboarding, performance optimization, and SIEM engineering across Cloud, On-Premise, and Hybrid environments. Strong in Linux administration, scripting (Python/Shell/PowerShell), and cloud platforms (AWS/Azure). Currently engineering large-scale data platforms at Mercado Libre.

TECHNICAL SKILLS

- **Splunk:** Indexer & Search Head Clustering (single-site and multi-site) · Splunk Cloud · SPL · Enterprise Security (ES) · SOAR · UBA · custom apps, add-ons, dashboards · CIM · field extractions (Regex).
- **Data Onboarding:** Universal Forwarder (UF) · HTTP Event Collector (HEC) · Syslog · DB Connect · REST API · data normalization & enrichment.
- **Platform & Data:** Splunk · Elastic Stack (ELK) · Linux/Unix administration · Windows Server · upgrades, troubleshooting, capacity planning · networking (TCP/UDP, HTTP, SSH).
- **Scripting & IaC:** Python · Shell · PowerShell · Terraform (Infrastructure as Code).
- **Cloud:** AWS (EC2, S3, ALB) · Azure.

PROFESSIONAL EXPERIENCE

Senior Cloud Cybersecurity Engineer

Apr 2025 – Present

Mercado Libre · Full-time

- Engineer a large-scale initiative migrating and unifying multiple legacy SIEM platforms (200+ data sources) into a unified, SOCless Security Data Lake, managing the lifecycle of petabytes of events (Hot/Warm/Cold/Frozen) on AWS (EC2/S3).
- Provision and manage ELK stack infrastructure through Terraform (IaC); administer the global agent fleet for resilient, standardized telemetry collection via Syslog, HTTP, and REST API.
- Orchestrate ingestion and normalization of native and custom data sources, enforcing strict schema mapping for data interoperability and detection fidelity.
- Developed AI agent–based pipelines (Python) that automate migration of 2,000+ detection rules across SIEM platforms—including quality control, metadata enrichment, MITRE ATT&CK mapping, and automated assessment of rule coverage and deprecation.
- Contributed to an AI-powered tool that detects MITRE ATT&CK/ATLAS coverage gaps and generates and tests new UEBA detection rules; built pipelines that validate existing detection rules and quarantine those that do not meet quality standards.
- SIEM focal point in compliance audits across multiple frameworks (BCRA, ISO 27001, PCI-DSS, and others): present and respond to auditors on the platform's logging, monitoring, retention, and SIEM coverage of segmented environments (e.g. the PCI/CDE scope), in both internal alignment reviews and with external auditors.
- Manage changes to the SIEM platform in regulated environments through formal change processes (RFC) with compliance approval prior to implementation.

Splunk Certified Instructor

Jan 2025 – Present

Splunk · Contract

- Official Splunk Certified Instructor (active role): currently deliver the Fast Start certification track preparing professionals for the Splunk Core Certified Power User certification—keeping platform expertise current and hands-on.

Splunk Engineer → Technical Leader
2020 – 2025

Target Minds · Full-time

- Progressed from Splunk Engineer (2020–2023) to Technical Leader (2023–2025), leading end-to-end design and implementation of scalable, distributed, clustered Splunk environments (Cloud, On-Premise, Hybrid) for clients across Banking, Finance, Energy, and Insurance.
- Managed the full Splunk platform lifecycle: upgrades, performance optimization, troubleshooting, and capacity planning for complex Indexer and Search Head clusters.
- Conducted data ingestion (including DB Connect), normalization (CIM), classification, and enrichment of complex data sources; developed custom add-ons and advanced field extractions (Regex).
- Worked extensively with Splunk Enterprise Security (ES) and MITRE ATT&CK mappings; implemented Splunk SOAR for automation and installed and configured Splunk UBA for behavioral threat detection.
- Integrated Splunk with external systems, cloud platforms, databases, and automation tools; led and mentored the technical team as Technical Leader.

Splunk Consultant
Feb 2023 – Aug 2024

CyberStone · Independent Contractor (part-time)

- Provided on-demand Splunk consulting in parallel with full-time work: issue resolution and platform troubleshooting for client environments.
- Performed threat hunting and forensic analysis during security incidents, using Splunk to investigate and support incident response.

PMO Analyst
Jan 2019 – Jul 2020

MetroGAS

- Built dashboards and project status reports (Python, Splunk, Power BI) to monitor a large SAP implementation and communicate complex data to stakeholders.

Senior Business Analyst
Feb 2011 – Jan 2019

Policía Federal Argentina

- Led project deliverables and translated business requirements into software specifications; maintained Oracle (PL/SQL) systems with batch processing, procedures, and triggers.

CERTIFICATIONS

- **Splunk:** Enterprise Certified Architect · Core Certified Consultant · Certified Instructor (active — currently delivering the official Core Power User track) · Enterprise Security Certified Admin · Cloud Certified Admin · Enterprise Certified Admin · Core Certified Power User · SOAR.
- **Cloud:** Microsoft Certified: Azure Fundamentals.

EDUCATION

Master's Degree, Data Science — Universidad CAECE (GPA 9, Graduated) 2020 – 2021

Bachelor's Degree — Universidad de Palermo (Graduated) 2014 – 2019