Leandro Federico Juárez

Splunk Consultant & Architect · SIEM Engineer · Instructor Certificado Splunk

Argentina (CABA/AMBA) | linkedin.com/in/leandrofjuarez | Inglés: Avanzado | Español: Nativo

PERFIL

Splunk Enterprise Certified Architect y Core Certified Consultant, con más de 12 años en IT y más de 5 años especializado en Splunk—y uno de los pocos profesionales acreditados también como Splunk Certified Instructor oficial, combinando experiencia profunda en arquitectura con dominio comprobado y vigente de la plataforma. Amplia experiencia hands-on en despliegues distribuidos y clusterizados (Indexer & Search Head Clustering), onboarding de datos, optimización de performance e ingeniería SIEM en entornos Cloud, On-Premise e Híbridos. Sólido manejo de administración Linux, scripting (Python/Shell/PowerShell) y plataformas cloud (AWS/Azure). Actualmente desarrollando plataformas de datos a gran escala en Mercado Libre.

HABILIDADES TÉCNICAS

- **Splunk:** Indexer & Search Head Clustering (single-site y multi-site) · Splunk Cloud · SPL · Enterprise Security (ES) · SOAR · UBA · apps, add-ons y dashboards personalizados · CIM · field extractions (Regex).
- **Onboarding de datos:** Universal Forwarder (UF) · HTTP Event Collector (HEC) · Syslog · DB Connect · REST API · normalización y enriquecimiento de datos.
- **Plataformas y datos:** Splunk · Elastic Stack (ELK) · administración Linux/Unix · Windows Server · upgrades, troubleshooting, capacity planning · redes (TCP/UDP, HTTP, SSH).
- **Scripting e IaC:** Python · Shell · PowerShell · Terraform (Infrastructure as Code).
- **Cloud:** AWS (EC2, S3, ALB) · Azure.

EXPERIENCIA PROFESIONAL

Senior Cloud Cybersecurity Engineer

abr. 2025 – actualidad

Mercado Libre · Jornada completa

- Trabajo en una iniciativa a gran escala de migración y unificación de múltiples plataformas SIEM legacy (200+ fuentes de datos) en una plataforma SOCless unificada (Security Data Lake), gestionando el ciclo de vida de petabytes de eventos (Hot/Warm/Cold/Frozen) en AWS (EC2/S3).
- Provisiono y administro infraestructura del stack ELK mediante Terraform (IaC); administro la flota global de agentes para una recolección de telemetría resiliente y estandarizada vía Syslog, HTTP y REST API.
- Orquesto la ingesta y normalización de fuentes de datos nativas y personalizadas, aplicando un mapeo de esquema estricto para garantizar interoperabilidad y fidelidad de detección.
- Desarrollé pipelines basados en agentes de IA (Python) que automatizan la migración de más de 2.000 reglas de detección entre plataformas SIEM—incluyendo control de calidad, enriquecimiento de metadata, mapeo a MITRE ATT&CK y evaluación automática de cobertura y deprecación de reglas.
- Contribuí a una herramienta basada en IA que detecta gaps de cobertura en MITRE ATT&CK/ATLAS y genera y prueba nuevas reglas de detección UEBA; construí pipelines que validan reglas de detección existentes y ponen en cuarentena las que no cumplen los estándares de calidad.
- Referente del SIEM en auditorías de cumplimiento para múltiples marcos normativos (BCRA, ISO 27001, PCI-DSS, entre otros): presento y respondo ante los auditores sobre logging, monitoreo, retención y la cobertura del SIEM sobre entornos segmentados (p. ej. el entorno PCI/CDE), tanto en instancias internas de alineación como ante auditores externos.
- Gestiono cambios sobre la plataforma SIEM en entornos regulados mediante procesos formales (RFC) con aprobación de compliance previa a su implementación.

Splunk Certified Instructor

ene. 2025 – actualidad

Splunk · Contrato

- Instructor certificado oficial de Splunk (rol activo): actualmente dicto el track de certificación Fast Start que prepara a profesionales para la certificación Splunk Core Certified Power User—manteniendo mi expertise en la plataforma vigente y práctico.

Splunk Engineer → Technical Leader
2020 – 2025

Target Minds · Jornada completa

- Progresé de Splunk Engineer (2020–2023) a Technical Leader (2023–2025), liderando el diseño e implementación end-to-end de entornos Splunk escalables, distribuidos y clusterizados (Cloud, On-Premise, Híbrido) para clientes de los sectores Banca, Finanzas, Energía y Seguros.
- Gestioné el ciclo de vida completo de la plataforma Splunk: upgrades, optimización de performance, troubleshooting y capacity planning para clusters complejos de Indexer y Search Head.
- Realicé ingesta de datos (incluyendo DB Connect), normalización (CIM), clasificación y enriquecimiento de fuentes de datos complejas; desarrollé add-ons personalizados y field extractions avanzadas (Regex).
- Trabajé extensamente con Splunk Enterprise Security (ES) y mapeos a MITRE ATT&CK; implementé Splunk SOAR para automatización e instalé y configuré Splunk UBA para detección de amenazas por comportamiento.
- Integré Splunk con sistemas externos, plataformas cloud, bases de datos y herramientas de automatización; lideré y guié al equipo técnico como Technical Leader.

Splunk Consultant
feb. 2023 – ago. 2024

CyberStone · Contractor independiente (part-time)

- Brindé consultoría Splunk a demanda en paralelo a mi trabajo full-time: resolución de issues y troubleshooting de plataforma para entornos de clientes.
- Realicé threat hunting y análisis forense durante incidentes de seguridad, utilizando Splunk para investigar y dar soporte a la respuesta a incidentes.

PMO Analyst
ene. 2019 – jul. 2020

MetroGAS

- Construí dashboards y reportes de estado de proyecto (Python, Splunk, Power BI) para monitorear una implementación SAP de gran escala y comunicar datos complejos a los stakeholders.

Senior Business Analyst
feb. 2011 – ene. 2019

Policía Federal Argentina

- Lideré entregables de proyecto y traduje requerimientos de negocio a especificaciones de software; mantuve sistemas Oracle (PL/SQL) con procesamiento batch, procedimientos y triggers.

CERTIFICACIONES

- **Splunk:** Enterprise Certified Architect · Core Certified Consultant · Certified Instructor (activa — dictando actualmente el track oficial Core Power User) · Enterprise Security Certified Admin · Cloud Certified Admin · Enterprise Certified Admin · Core Certified Power User · SOAR.
- **Cloud:** Microsoft Certified: Azure Fundamentals.

EDUCACIÓN

Maestría en Ciencia de Datos — Universidad CAECE (Promedio 9, Graduado) 2020 – 2021

Licenciatura — Universidad de Palermo (Graduado) 2014 – 2019