# Shon Caspy

Target: Ingeniero/a - Especialista SIEM & SOAR

Madrid, Spain | narubian@gmail.com | +34 627 28 09 95 | linkedin.com/in/shon-caspy

## Summary

Profesional de operaciones tecnológicas especializado en Splunk, análisis de logs y automatización de recuperación mediante APIs en banca digital. Experiencia en consultas SPL, correlación con Regex, dashboards y diagnóstico de integraciones, con resultados de reducción de alertas de hasta el 90% mediante recuperación, supresión aprobada y correcciones de ingeniería. Aporta gestión de equipos pequeños, mentoría técnica y soporte B2B de Microsoft 365, con una satisfacción del cliente de aproximadamente 4,9/5.

## Technical Skills

Log Management: Splunk, SPL y Regex: procesamiento, normalización y correlación de registros; investigación por lotes, reconstrucción de datos y validación de cobertura.

Alertas y casos de uso: Configuración de alertas avanzadas; Desarrollo de casos de uso complejos: detección de fallos operativos, clasificación de errores y comprobación de correlaciones.

Visualización: Creación de dashboards y reportes: KPIs de salud de plataforma en Splunk, vistas operativas en ServiceNow y exportaciones CSV según necesidades de stakeholders.

Scripting y automatización: Postman, REST APIs y JSON para recuperación; Python en pruebas de concepto; PowerShell para diagnóstico de Microsoft 365; LangGraph en proyectos personales asistidos por agentes.

Gestión de incidentes: Level 2 technical support en ServiceNow; respuesta ante incidentes operativos mediante diagnóstico de integraciones MuleSoft, recuperación y coordinación con equipos responsables.

Controles de ciberseguridad: Identity and access management en soporte Microsoft 365 SaaS: permisos efectivos, grupos y RBAC; diagnóstico de autenticación de correo mediante SPF y DMARC.

Documentación y colaboración: Runbooks y pruebas técnicas en Confluence; traducción de requisitos a KPIs; Git y GitLab para cambios asignados con revisión previa a producción.

Desarrollo de equipos: Liderazgo de equipos técnicos: asignación de tareas en una función de tres personas; Mentoría y capacitación mediante acompañamiento práctico y resolución guiada.

## Professional Experience

**Information Technology Operations Specialist** | **Western Union**
August 2023 - February 2026

- Construí la detección y vista Splunk de fallos de vinculación de tarjetas y una colección Postman para recuperarlos mediante REST APIs encadenadas. Un CSV exportado manualmente conectaba ambos pasos; el equipo L2 adoptó la colección en aproximadamente dos días.
- En ese mismo trabajo, demostré una clasificación de errores en tres vías mediante SPL y Regex, documentada en Confluence. Coordiné la supresión aprobada con BigPanda y mi responsable, y la corrección con Mambu: alertas reducidas primero un 80% y después un 90%.
- Desarrollé dashboards Splunk para responsables de ingeniería con tasas de error, altas por hora y día, y volúmenes e importes de transacciones por país. Traduje necesidades de KPIs a datos disponibles y normalicé formatos heterogéneos mediante Regex.
- Automaticé la identificación de reejecuciones de facturación tras el traslado local de un microservicio MuleSoft, utilizando Regex para analizar diez archivos de logs con mensajes inconsistentes y contrastar éxitos y fallos con el Excel de origen.
- Reconstruí desde Splunk el conjunto completo identificado tras una interrupción de escritura en Snowflake de aproximadamente un mes. Verifiqué repetidamente su integridad y preparé los campos solicitados para que el equipo responsable ejecutara la reintroducción.
- Atendí incidentes L2 en ServiceNow, rastreando logs hasta código y flujos MuleSoft para localizar fallos entre sistemas. En incidentes mayores aporté evidencia sobre la salud de los servicios de orquestación y su afectación.

**L2 Operations Support** | **NEO (getneo.com)**
November 2022 - February 2023

- Escribí consultas SQL para conciliación de libros, validación de consistencia e investigación de discrepancias entre varios sistemas financieros durante una asignación breve.
- Desarrollé una prueba de concepto en Python que conectaba Slack con Azure DevOps Work Items para automatizar la creación interna de tickets.

**Technical Support Engineer** | **Teleperformance**
April 2021 - February 2022

- Mantuve una satisfacción del cliente de aproximadamente 4,9/5 atendiendo varios cientos de casos semanales de administradores Microsoft 365, incluidos problemas complejos y situaciones de alta fricción en un equipo muy limitado de personal.
- Presté soporte B2B de Microsoft 365 SaaS a administradores: Azure Active Directory, Intune, permisos, licencias, Exchange, recuperación de buzones, retención, OneDrive y almacenamiento SharePoint.
- Utilicé PowerShell para localizar un buzón inesperado y corregir su asociación con la cuenta Azure Active Directory, resolviendo una migración fallida. Investigué también permisos superpuestos, herencia de grupos y RBAC.
- Orienté a administradores en configuraciones híbridas y migraciones entre entornos locales y cloud. Durante la formación Microsoft 365, ayudé al responsable del equipo con ejercicios y acompañé técnicamente a la segunda incorporación formativa.

**Information Technology Team Manager** | **Centro Medico La Paz**
August 2020 - May 2021

- Gestioné una función de TI de tres personas en un complejo hospitalario, asignando intervenciones y desarrollando la autonomía de un técnico mediante preguntas e indicaciones durante casos reales.
- Recuperé el servidor Exchange tras un fallo de configuración y realicé recuperaciones de buzones con AOMEI Backupper y NAS propio, gestionando manualmente la capacidad disponible.
- Administré DNS y DHCP en Windows Server, manteniendo coherentes direcciones y registros; edité GPO existentes y configuré SPF y DMARC para el correo del complejo.

**Service Engineer** | **MAR Ltd**
March 2016 - January 2020

- Presté soporte remoto a médicos y personal administrativo, incluida cobertura fuera de horario, resolviendo servicios clínicos bloqueados y reparando relaciones entre exámenes, imágenes y transcripciones en DICOM/PACS y RIS.
- Participé en la construcción de una aplicación de tickets C# .NET con almacenamiento XML, preparando personalmente el servidor local para que usuarios y TI registraran y siguieran solicitudes.

**End User Support Specialist** | **HOT Telecommunication**
January 2010 - January 2011

- Resolví fallos de conectividad por teléfono, distinguiendo problemas de línea, router y equipo mediante IP, DHCP, ping y traceroute, y manteniendo conversaciones difíciles hasta su resolución.

## Personal Projects

**Personal AI Automation & Local Inference Portfolio (Personal Project)**

- En proyectos personales, definí arquitecturas y criterios de aceptación para automatizaciones Python y LangGraph con asistencia material de agentes, utilizando estados tipados, nodos, condiciones y validaciones.
- Redacté 47 procedimientos operativos y 24 habilidades ejecutables para agentes, incorporando selección de modelos y controles de verificación; diseñé comprobaciones de procedencia, conciliación y éxito o fallo.

## Education

**The Hebrew Reali School**, GED, Computer Programming + Physics
July 2011