Shon Caspy

Target: Administrador SIEM (Ciberseguridad)

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

Summary

Profesional de operaciones IT en Madrid con experiencia en Splunk, análisis de logs y Level 2 technical support en banca digital. Desarrolla casos de uso de monitorización operativa, alertas, dashboards y automatizaciones de recuperación, con investigación de fallos entre microservicios y proveedores. Aporta además soporte B2B de Microsoft 365, documentación técnica, atención de escalados y experiencia en telecomunicaciones.

Technical Skills

Splunk: SPL, Regex, vistas, alertas y dashboards; creación de casos de uso desde cero para monitorización operativa y validación de resultados.

Análisis de logs: Parsing, correlación por identificadores, normalización de campos, reconstrucción de datos y comprobación de integridad.

Operaciones L2: gestión de incidencias e investigación de incidentes operativos; ServiceNow, diagnóstico de causa raíz y coordinación de correcciones.

Automatización y documentación: Postman, REST APIs, JSON, CSV y Python; procedimientos de recuperación y runbooks en Confluence.

Identidad y acceso: Microsoft 365 SaaS, Azure Active Directory, permisos, grupos, RBAC, Intune y PowerShell; autenticación de correo SPF y DMARC.

Infraestructura y telecomunicaciones: Windows Server, DNS, DHCP, edición de GPO, Exchange y backups; conectividad TCP/IP, configuración remota de CPE y coadministración SIP/VoIP.

Professional Experience

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

- Creó la alerta y vista Splunk para detectar fallos de vinculación de tarjetas y una colección Postman que encadenaba llamadas REST y variables JSON para recuperarlos. Conectó ambos mediante exportación CSV manual; el equipo L2 utilizó la colección en unos dos días.
- En esa misma solución, demostró con SPL y Regex una clasificación de tres tipos de error, documentada en Confluence. Coordinó la supresión con BigPanda y su responsable, y la corrección con Mambu; las alertas bajaron un 80% y posteriormente un 90%.
- Construyó dashboards y alertas Splunk para responsables de ingeniería: tasas de error, altas por hora y día, transacciones e importes por país. Unificó formatos heterogéneos mediante Regex y tradujo necesidades de stakeholders en KPIs calculables con los datos disponibles.
- Atendió tickets L2 en ServiceNow, correlacionando logs y trazando código MuleSoft para localizar fallos entre servicios y proveedores. Durante incidentes mayores aportó evidencia sobre la salud de los servicios de orquestación y si estaban afectados.
- Reconstruyó en Splunk el conjunto identificado de datos afectados por una interrupción de escritura en Snowflake de aproximadamente un mes. Verificó repetidamente su integridad y preparó los campos solicitados por el equipo responsable para su posterior reencolado.
- Automatizó la identificación de reejecuciones necesarias en la facturación mensual tras el traslado local de un microservicio MuleSoft. Aplicó Regex sobre diez archivos de logs inconsistentes y contrastó éxitos y fallos con el Excel de origen.

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

- Escribió consultas SQL para conciliación de libros y validación de consistencia entre sistemas financieros, investigando discrepancias mediante consultas sobre los datos.
- Desarrolló un bot Python como prueba de concepto que conectaba Slack con Azure DevOps Work Items para automatizar la creación de tickets internos.

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

- Mantuvo una satisfacción de clientes de aproximadamente 4,9/5 mientras atendía varios cientos de casos semanales de administradores Microsoft 365, incluidos problemas complejos y de alta fricción, en un equipo con recursos limitados.
- Prestó soporte B2B sobre Microsoft 365 SaaS: Azure Active Directory, Intune, permisos, licencias, Exchange Online, OneDrive y SharePoint. Investigó conflictos de herencia entre grupos y diseño de grupos de roles RBAC.
- Resolvió una migración de correo fallida identificando mediante PowerShell un buzón inesperado y asociándolo a la cuenta correcta. También orientó a administradores en configuraciones híbridas y migraciones de Exchange e identidad.
- Actuó como referente técnico y punto de escalado, proporcionando estrategias de diagnóstico a compañeros y especialistas. Durante la formación de Microsoft 365 ayudó con ejercicios prácticos y mentorizó a la siguiente incorporación de alumnos.
- Diagnosticó y corrigió fallos de autenticación SPF y DMARC que enviaban correo legítimo a spam. Guio a clientes mediante consultas DNS y revisión de registros, registradores y servidores de nombres.

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

- Gestionó un equipo IT de tres personas en un recinto hospitalario, asignando tareas y orientando a un técnico durante incidencias para desarrollar su autonomía.
- Recuperó el servidor Exchange tras un fallo de configuración y realizó restauraciones de buzones con AOMEI Backupper. Mantuvo el NAS y su capacidad sin herramientas de pago.
- Administró DNS y DHCP coordinando direcciones y registros; editó GPO existentes y configuró SPF y DMARC. Mantuvo PCs e impresoras mediante reparación y sustitución de componentes.

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

- Proporcionó soporte remoto a médicos y personal administrativo, incluida cobertura fuera de horario. Resolvió bloqueos de servicios clínicos e impresoras de CD para restablecer sus flujos de trabajo.
- Reparó relaciones huérfanas entre exploraciones, imágenes y transcripciones en un entorno DICOM/PACS y RIS, restableciendo la vinculación correcta de los registros clínicos.
- Colaboró en una aplicación de tickets C# .NET para IT y usuarios, preparando personalmente el servidor local; la solución permitía registrar y seguir solicitudes de soporte.

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

- Resolvió incidencias telefónicas de banda ancha y desescaló clientes frustrados. Aisló fallos entre línea, router y PC mediante direccionamiento IP, ping y traceroute, y configuró remotamente CPE, DHCP, Wi-Fi y firmware.

Personal Projects

Personal AI Automation & Local Inference Portfolio (Personal Project)

- En su portfolio personal, redactó 47 procedimientos operativos para agentes y 24 habilidades ejecutables, incorporando selección de modelos y controles de verificación.

CCNA network fundamentals coursework (Personal Project)

- Estudió aproximadamente el 40% de un curso CCNA, hasta direccionamiento y subnetting: cableado, octetos, cálculo binario y distribución de subredes y hosts.

Education

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