Shon Caspy

Target: Administrador/a SIEM (Ciberseguridad)

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

Summary

Profesional de operaciones IT con experiencia práctica en Splunk, análisis de logs, correlación, alertas y desarrollo de casos de uso operativos en banca digital. Combina soporte técnico de segundo nivel, automatización de recuperaciones mediante APIs y experiencia en telecomunicaciones. En soporte Microsoft 365 para administradores mantuvo un CSAT de aproximadamente 4,9/5.

Technical Skills

Splunk: SPL, Regex, búsquedas, extracción y normalización de campos, correlación de eventos, dashboards y validación de datos.

Casos de uso operativos: Creación de vistas y reglas de alerta; clasificación de errores, detección de fallos y reducción de ruido.

Diagnóstico e incidentes: Level 2 technical support: ServiceNow, análisis de causa raíz, trazabilidad de flujos MuleSoft y evaluación del estado de servicios.

Automatización y datos: Postman, REST APIs, JSON, CSV, SQL y Python; encadenamiento de peticiones y cambios puntuales con Git/GitLab.

Identidad y seguridad de acceso: Soporte B2B de Microsoft 365 SaaS: Azure Active Directory, Intune, permisos, grupos, RBAC y autenticación SPF/DMARC.

Infraestructura y telecomunicaciones: Windows Server, DNS, DHCP, TCP/IP, configuración remota de CPE, conectividad de banda ancha y coadministración SIP/VoIP.

Documentación y colaboración: Runbooks en Confluence, documentación de pruebas, coordinación con equipos técnicos, orientación a administradores y mentoría práctica.

Professional Experience

Information Technology Operations Specialist | **Western Union**

August 2023 - February 2026

- Definí alertas y construí una vista Splunk para detectar fallos de vinculación de tarjetas. Exporté los identificadores mediante CSV a una colección Postman propia que encadenaba REST APIs para recuperarlas; el equipo L2 comenzó a utilizarla en unos dos días.
- En ese mismo trabajo, demostré con SPL y Regex una clasificación de errores en tres categorías, documentada en Confluence. Coordiné la supresión con BigPanda y mi responsable, y la corrección de código con ingeniería de Mambu: las alertas bajaron un 80% y posteriormente un 90%.
- Construí dashboards Splunk para responsables de ingeniería con tasas de error, altas y transacciones por país. Normalicé formatos mediante Regex y creé alertas para flujos sin éxitos durante intervalos anómalos, traduciendo necesidades de seguimiento a indicadores disponibles.
- Investigué incidentes de ServiceNow como soporte de segundo nivel, siguiendo logs hasta el código MuleSoft y sus flujos entre sistemas. En reuniones de incidentes mayores aporté evidencia sobre la salud y afectación de los servicios de orquestación.
- Reconstruí en Splunk el conjunto identificado de datos afectados por una interrupción de escritura en Snowflake de aproximadamente un mes. Comprobé su integridad y preparé los campos solicitados para que el equipo responsable ejecutara el reprocesamiento.
- Automaticé la identificación de reejecuciones de facturación analizando diez archivos de logs locales con Regex y contrastando éxitos y fallos con el Excel de origen, sustituyendo búsquedas manuales prolongadas.

L2 Operations Support | **NEO (getneo.com)**

November 2022 - February 2023

- Escribí consultas SQL para conciliación de registros y validación de consistencia entre sistemas financieros. Desarrollé un prototipo Python que conectaba Slack con Azure DevOps Work Items para crear tickets internos.

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

- Mantuve un CSAT de aproximadamente 4,9/5 al resolver casos complejos de administradores Microsoft 365 bajo una carga sostenida de varios cientos de casos semanales en un equipo con dotación insuficiente.
- Presté soporte B2B sobre Azure Active Directory, Intune, licencias, grupos, Exchange Online, OneDrive y SharePoint; investigué permisos superpuestos, herencia de grupos y configuración de roles RBAC.
- Resolví una migración de buzón bloqueada utilizando PowerShell para localizar un buzón inesperado y asociarlo a la cuenta correcta. También diagnostiqué problemas de autenticación SPF/DMARC que alteraban el enrutamiento del correo.
- Guié a administradores en configuraciones híbridas y migraciones de entornos locales a Microsoft 365. Durante la formación de admin centers ayudé con ejercicios y PowerShell, y acompañé técnicamente a la siguiente incorporación de alumnos.

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

- Gestioné un equipo IT de tres personas en un recinto hospitalario, asignando tareas y manteniendo PCs e impresoras con repuestos escasos; orienté a un técnico durante incidencias para desarrollar su autonomía.
- Administré DNS y DHCP en Windows Server, manteniendo coherencia entre direcciones estáticas y registros de equipos. Modifiqué GPO existentes y configuré registros SPF/DMARC del correo.
- Gestioné copias con AOMEI Backupper y almacenamiento NAS; recuperé buzones y restauré el servidor Exchange tras un fallo de configuración, restableciendo el correo sin herramientas de pago ni soporte del proveedor.

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

- Proporcioné soporte remoto a médicos y personal administrativo, incluida cobertura fuera de horario. Resolví bloqueos de servicios clínicos y reparé relaciones entre exámenes, imágenes y transcripciones en DICOM/PACS y RIS.
- Administré DNS/DHCP y coadministré telefonía SIP/VoIP. Colaboré en una aplicación de tickets C# .NET, instalando personalmente el servidor local que sustentaba el registro compartido de solicitudes.

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

- Resolví incidencias telefónicas de banda ancha, diferenciando fallos de línea, router y equipo mediante direcciones IP, DHCP, ping, traceroute y pruebas de velocidad; acompañé a clientes frustrados hasta la resolución.
- Configuré CPE remotamente desde la consola del proveedor: SSID, claves Wi-Fi, DHCP, redirección de puertos, filtros MAC, credenciales PPPoE y firmware.

Education

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