Shon Caspy

Target: Ingeniero/a - Especialista SIEM & SOAR Microsoft Sentinel, Crowdstrike, XSIAM y Splunk

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

Summary

Especialista en operaciones y soporte técnico de nivel 2 con experiencia profesional en Splunk, análisis de logs, dashboards y automatización de recuperación mediante APIs REST. Desarrolló consultas, alertas y documentación operativa, contribuyendo a reducir alertas un 80% y después un 90% mediante recuperación, supresión aprobada y correcciones de ingeniería. Aporta soporte B2B de Microsoft 365 con aproximadamente 4,9/5 de CSAT, diagnóstico de identidades y permisos, gestión de equipos y mentoría práctica.

Technical Skills

Log Management; Splunk: Búsqueda, extracción, normalización y correlación operativa de logs; consultas SPL, Regex, alertas y dashboards personalizados según requisitos de responsables de ingeniería.

automatización; Automatización y gestión de logs mediante scripting: Procesamiento con SPL y Regex, identificación de reejecuciones y recuperación mediante Postman, encadenamiento de APIs REST, variables JSON y lotes CSV.

Level 2 technical support; Análisis técnico: Investigación de incidencias en ServiceNow, diagnóstico de causa raíz, trazado de integraciones MuleSoft, validación de datos y documentación de hallazgos en Confluence.

Conocimientos básicos en ciberseguridad: Seguridad de identidades y accesos: permisos, grupos, herencia y RBAC en Azure Active Directory y Microsoft 365; autenticación de correo mediante SPF y DMARC.

Python y PowerShell: Python aplicado a un bot Slack–Azure DevOps como prueba de concepto; PowerShell utilizado para diagnóstico y administración de Exchange y Azure Active Directory.

Liderazgo de equipos técnicos; Mentoría y capacitación: Gestión de un equipo de TI de tres personas, asignación de tareas, acompañamiento técnico durante incidencias y mentoría informal en formación Microsoft 365.

Comunicación y trabajo en equipo: Atención a administradores empresariales, resolución de casos complejos y colaboración con equipos internacionales, responsables técnicos e ingeniería para aplicar correcciones y mejoras operativas.

Inglés técnico intermedio o superior: Inglés nativo, C1/C2, utilizado diariamente en comunicaciones, soporte técnico y atención a clientes.

Professional Experience

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

- Creó la alerta y vista Splunk para detectar tarjetas sin vincular; exportó identificadores mediante CSV y construyó una colección Postman para recuperación por lotes mediante APIs REST. El equipo L2 comenzó a utilizarla en aproximadamente dos días.
- En esa misma mejora, documentó una clasificación de errores de tres vías mediante SPL, Regex y Confluence para obtener aprobación de supresión. Coordinó BigPanda, su responsable y los ingenieros Mambu que implementaron la corrección: alertas reducidas un 80%, después un 90%.
- Desarrolló casos de uso operativos y dashboards de salud de plataforma: tasas de error, incorporaciones y transacciones por país. Tradujo necesidades de stakeholders a KPIs disponibles, normalizó formatos mediante Regex y creó alertas por ausencia prolongada de operaciones satisfactorias.
- Automatizó la identificación de reejecuciones de facturación mediante Regex sobre diez archivos locales de logs con mensajes inconsistentes, contrastando éxitos y fallos con el Excel de origen tras el traslado local de un microservicio MuleSoft.
- Investigó incidencias de segunda línea en ServiceNow, relacionando correlaciones y eventos Splunk con código MuleSoft y flujos entre proveedores. En salas de crisis, aportó evidencias de logs y métricas para determinar si los servicios de orquestación estaban afectados.
- Reconstruyó desde 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 receptor para su posterior reencolado.

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

- Escribió consultas SQL para reconciliar libros de transacciones, validar consistencia de datos e investigar discrepancias entre sistemas financieros.
- 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 aproximadamente 4,9/5 de CSAT mientras atendía varios cientos de casos semanales de administradores Microsoft 365 en un equipo con fuerte escasez de personal y resolvía problemas complejos y de elevada fricción.
- Prestó soporte B2B de Microsoft 365 SaaS sobre Azure Active Directory, Intune, licencias, grupos, Exchange Online, retención, OneDrive y SharePoint, además de problemas de Outlook y cuentas en Windows 10/11.
- Resolvió problemas no documentados de permisos superpuestos, herencia de grupos y RBAC. Utilizó PowerShell para localizar un buzón inesperado, asociarlo a la cuenta correcta y resolver una migración fallida.
- Diagnosticó fallos de autenticación de correo relacionados con SPF y DMARC; orientó a administradores en configuraciones híbridas y migraciones entre servidores locales y Microsoft 365, corrigiendo problemas en la frontera entre ambos entornos.
- Fue referencia técnica durante la formación de centros de administración Microsoft 365, guio ejercicios de conexión PowerShell a Exchange Online y acompañó a la segunda incorporación durante su formación.

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

- Gestionó un equipo de TI de tres personas en un complejo hospitalario; asignó intervenciones y desarrolló la autonomía de un técnico mediante preguntas y pistas durante la resolución de incidencias.
- Recuperó el servidor Exchange tras un fallo de configuración y realizó recuperaciones de buzones con AOMEI Backupper gratuito; mantuvo el NAS y gestionó manualmente su capacidad.
- Administró DHCP y DNS manteniendo coherencia entre direcciones y registros; editó GPO existentes según las necesidades de configuración de los equipos.

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

- Prestó soporte remoto a médicos y personal administrativo, con cobertura fuera de horario; resolvió bloqueos de servicios clínicos y reparó relaciones entre exámenes, imágenes y transcripciones en DICOM/PACS y RIS.
- Ejecutó cambios probados localmente y respaldos incrementales en producción; colaboró en una aplicación de tickets C# .NET, instalando personalmente el servidor local para registrar y seguir solicitudes.

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

- Diagnosticó fallos de conectividad por teléfono mediante configuración IPv4, ping y traceroute; configuró routers remotamente y desescaló llamadas hasta resolver el problema.

Personal Projects

Personal AI Automation & Local Inference Portfolio (Personal Project)

- En su portfolio personal, redactó 47 procedimientos operativos y 24 habilidades ejecutables para agentes, con selección de modelos y controles de verificación.
- Definió arquitecturas y criterios de aceptación para automatizaciones personales LangGraph con asistencia de agentes de programación; evaluó resultados mediante pruebas, scorecards y comprobaciones explícitas de éxito o fallo.

CCNA network fundamentals coursework (Personal Project)

- Formación parcial CCNA: aproximadamente el 40% del curso, centrado en cableado, direccionamiento y cálculo de subredes; sin certificación.

Education

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