Shon Caspy

Target: Ingeniero Ciberseguridad SIEM/SOAR

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

Summary

Operations and technical support specialist with substantial Splunk experience spanning log analysis, operational monitoring, alert development and API recovery automation in digital banking. Combines validated false-positive classification, Python integration prototyping and systems troubleshooting with Microsoft 365 administrator advisory, cross-team problem resolution and approximately 4.9/5 customer satisfaction. English B2: English: Native, C1/C2. Systems and networking: Windows Server, DNS/DHCP administration, SMB routing and wireless support, and TCP/IP troubleshooting. Log parsing and normalization: Regex-based log parsing and normalization of inconsistent formats into common Splunk fields. Cloud environments: Cloud-environment experience through AWS monitoring and Microsoft 365 tenant and hybrid support; personal SaaS deployment. Scripting for task automation: Python scripting for a ticket-creation automation proof of concept; agent-assisted personal workflow automation.

Technical Skills

Splunk and monitoring: SPL searches, operational use cases, correlation-ID analysis, dashboards, alert rules and classification of false positives.

Log parsing and normalization: Regex parsing, normalization into common Splunk fields, structured recovery datasets and observed-population completeness validation.

Scripting for task automation: Python integration prototyping; Postman REST API chaining, JSON handling and batch operational recovery; PowerShell-based troubleshooting.

Systems and networking: Windows Server, DNS/DHCP, TCP/IP troubleshooting, SMB routers, wireless access, port forwarding and existing Group Policy editing.

Cloud environments: AWS performance monitoring; Microsoft 365 cloud and hybrid support; Azure Active Directory troubleshooting. Familiarity with Amazon CloudWatch and Amazon S3.

Identity and administrator support: Microsoft 365 SaaS, permissions, nested groups, RBAC, licensing, Intune, Exchange Online and SPF/DMARC diagnostics.

Documentation and collaboration: Confluence runbooks, ServiceNow Level 2 technical support, technical mentoring, engineering coordination and occasional reviewed Git/GitLab production changes.

English B2 requirement: English: Native, C1/C2; used daily for professional communication and customer service.

Professional Experience

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

- Built the connected card-link detection and recovery workflow: defined alerts, created a Splunk view of card/user identifiers, manually exported CSV and developed a Postman collection chaining REST APIs for batch recovery. The L2 team adopted the collection within about two days.
- For the same programme, proved three-way error classification with SPL, Regex and a Confluence runbook, securing BigPanda suppression approval. Coordinated suppression with the owning teams and supplied Mambu engineers with root-cause evidence; alerts fell 80%, then 90%, through the combined work.
- Developed Splunk dashboards and operational monitoring use cases around stakeholder KPIs: error rates, onboarding activity and transaction totals by country. Consolidated inconsistent formats into common fields and created alerts for flows with unusually prolonged gaps between successes.
- Automated identification of invoice-generation reruns by applying complex Regex across ten inconsistently phrased local logs and matching successes and failures against the source Excel file.
- Reconstructed the complete identified affected dataset after a roughly month-long Snowflake write gap. Searched Splunk, repeatedly checked completeness and parsed log chunks into the downstream team's requested fields for requeue.
- Investigated ServiceNow incidents through logs and MuleSoft source code, tracing upstream/downstream boundaries to identify responsible teams. Reported orchestration service health from live metrics during major-incident war rooms.

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

- Developed a Python proof-of-concept integration connecting Slack with Azure DevOps Work Items to automate internal ticket creation.
- Wrote substantial SQL queries for ledger reconciliation, data validation and query-based investigation of discrepancies across financial systems.

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

- Delivered B2B Microsoft 365 Concierge support primarily to tenant administrators, sustaining approximately 4.9/5 CSAT while handling several hundred administrator cases weekly in a severely understaffed team.
- Troubleshot overlapping permissions, nested-group inheritance and RBAC role groups. Used PowerShell to identify an unexpectedly named cloud mailbox and correct its Azure Active Directory account association, resolving a repeatedly failing migration.
- Supported Intune, licensing, Exchange recovery, retention, OneDrive, SharePoint, Outlook and Windows 10/11 account issues. Guided customer administrators through hybrid configurations and cloud migrations, and corrected SPF/DMARC-related mail-routing failures.
- Became a technical reference during the Microsoft 365 admin-center course, guided the team manager through exercises and mentored the following intake using practical PowerShell and cloud-storage demonstrations.

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

- Managed a three-person hospital IT function, assigned technician tasks and coached one technician toward independent resolution while maintaining PCs and printers under severe replacement-part scarcity.
- Administered Windows Server DNS/DHCP configurations, kept machine addresses and records aligned, edited existing Group Policy Objects and configured SPF/DMARC records.
- Maintained AOMEI Backupper backups on self-managed NAS storage, recovered mailboxes and restored the Exchange server after a configuration failure, recovering mail service without paid tooling or vendor support.

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

- Provided remote-desktop support and off-hours coverage for doctors and medical secretaries, resolving frozen clinical services and printing blockers; repaired orphaned DICOM/PACS examination-to-transcription relationships.
- Helped build a C# .NET ticketing application, personally establishing its local server and giving IT staff and end users a shared route for raising and tracking requests.

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

- Diagnosed consumer connectivity faults using IP configuration, ping, traceroute and line sampling; remotely configured customer routers and de-escalated frustrated callers through resolution.

Personal Projects

Personal AI Automation & Local Inference Portfolio (Personal Project)

- In personal projects, authored 47 agent SOPs and 24 executable skills with verification gates. Directed agent-assisted Python/LangGraph workflows, defining architecture, acceptance constraints and explicit validation checks.

CCNA network fundamentals coursework (Personal Project)

- Studied approximately 40% of CCNA coursework, covering cabling, addressing and subnetting arithmetic; course incomplete and no certification obtained.

Education

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

Languages

Fluent English (Native)